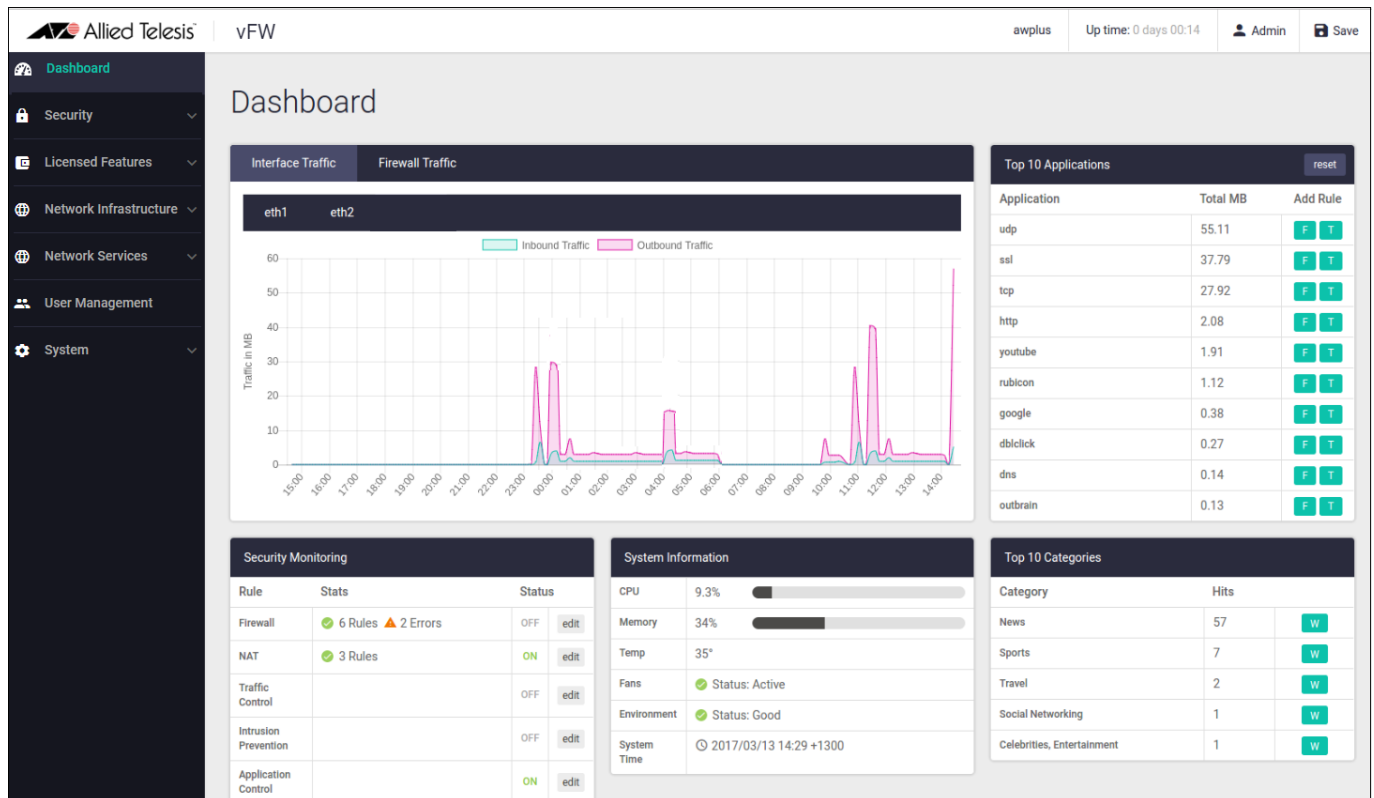


AR4000S-Cloud

ADVANCED VIRTUAL UTM FIREWALL



Command Reference for AlliedWare Plus™ Version 5.5.4-2.x

Acknowledgments

This product includes software developed by the University of California, Berkeley and its contributors.
Copyright ©1982, 1986, 1990, 1991, 1993 The Regents of the University of California.
All rights reserved.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For information about this see www.openssl.org/
Copyright (c) 1998-2019 The OpenSSL Project
Copyright (c) 1995-1998 Eric A. Young, Tim J. Hudson
All rights reserved.

For the full list of acknowledgments, and respective copyright notices, run the **show version** command on your device.

This product includes software licensed under v2 and v3 of the GNU General Public License, available from: www.gnu.org/licenses/gpl2.html and www.gnu.org/licenses/gpl.html respectively.

Source code for all GPL licensed software in this product can be obtained from the Allied Telesis GPL Code Download Center at: www.alliedtelesis.com/support/

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in Allied Telesis products, please send us a request by registered mail including a check for US\$15 to cover production and shipping costs and a CD with the GPL code will be mailed to you.

GPL Code Request
Allied Telesis Labs (Ltd)
PO Box 8011
Christchurch
New Zealand

Allied Telesis, AlliedWare Plus, Allied Telesis Management Framework, EPSRing, SwitchBlade, VCStack, and VCStack Plus are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc.

Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. All other product names, company names, logos or other designations mentioned herein may be trademarks or registered trademarks of their respective owners.

© 2025 Allied Telesis, Inc.

All rights reserved. No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

PART 1:	Setup and Troubleshooting	98
Chapter 1:	CLI Navigation Commands	99
	Introduction	99
	configure terminal	100
	disable (Privileged Exec mode)	101
	do	102
	enable (Privileged Exec mode)	103
	end	105
	exit	106
	help	107
	logout	108
	show history	109
Chapter 2:	Device GUI and Vista Manager EX Commands	110
	Introduction	110
	atmf topology-gui enable	111
	http log webapi-requests	112
	http port	113
	http secure-port	114
	http trustpoint	115
	log event-host	117
	service http	118
	show http	119
Chapter 3:	File and Configuration Management Commands	120
	Introduction	120
	boot config-file	123
	boot config-file backup	124
	boot system	125
	boot system backup	126
	cd	127
	copy (filename)	128

copy debug	130
copy running-config	131
copy startup-config	132
copy zmodem	133
delete	134
delete debug	135
dir	136
edit	138
erase factory-default	139
erase startup-config	140
ip tftp source-interface	141
ipv6 tftp source-interface	142
mkdir	143
move	144
move debug	145
pwd	146
rmdir	147
show boot	148
show hash	149
show file	150
show file systems	151
show running-config	153
show running-config interface	156
show running-config unencrypted	158
show startup-config	159
show version	160
software-upgrade	161
strict-user-process-control	162
strict-user-process-control force	163
write file	164
write memory	165
write terminal	166

Chapter 4:	User Access Commands	167
	Introduction	167
	aaa authentication enable default local	169
	aaa local authentication attempts lockout-time	170
	aaa local authentication attempts max-fail	171
	aaa login fail-delay	172
	clear aaa local user lockout	173
	clear line vty	174
	enable password	175
	enable secret (deprecated)	177
	exec-timeout	178
	length (asyn)	179
	line	180
	privilege level	181
	security-password history	182
	security-password forced-change	183
	security-password lifetime	184
	security-password min-lifetime-enforce	185
	security-password minimum-categories	186
	security-password minimum-length	187

	security-password reject-expired-pwd	188
	security-password warning	189
	service advanced-vty	190
	service password-encryption	191
	service telnet	192
	show aaa local user locked	193
	show privilege	195
	show security-password configuration	196
	show security-password user	197
	show telnet	198
	show users	199
	strict-user-process-control	200
	strict-user-process-control force	201
	telnet	202
	telnet server	203
	terminal length	204
	terminal resize	205
	username	206
Chapter 5:	Subscription Licensing Commands	208
	Introduction	208
	license update file	209
	license update online	210
	show license external	211
Chapter 6:	Update Manager Commands	212
	Introduction	212
	show resource	213
	update now	215
Chapter 7:	Web Redirect Commands	216
	Introduction	216
	browser-only (web-redirect)	217
	enable (web-redirect)	218
	exclude app	219
	exclude dst-ip	221
	exclude ip	223
	exclude mac	224
	exclude url	225
	idle-time (web-redirect)	227
	mode (web-redirect)	229
	proxy-host (web-redirect)	231
	repeat-time (web-redirect)	233
	server-url (web-redirect)	234
	show running-config web-redirect	235
	show web-redirect	236
	web-redirect	237
Chapter 8:	System Configuration and Monitoring Commands	238
	Introduction	238
	banner display external-manager	240
	banner exec	241

banner external-manager	243
banner login (system)	245
banner motd	247
clock summer-time date	249
clock summer-time recurring	251
clock timezone	253
debug core-file	254
hostname	255
low-memory restart	257
max-fib-routes	258
max-static-routes	259
no debug all	260
reboot	262
reload	263
show banner external-manager	264
show clock	265
show cpu	267
show cpu history	270
show debugging	272
show memory	273
show memory allocations	275
show memory history	277
show memory pools	278
show memory shared	279
show process	280
show reboot history	282
show router-id	283
show system	284
show system mac	285
show system serialnumber	286
show tech-support	287
terminal monitor	289
undebg all	290

Chapter 9:	Logging Commands	291
	Introduction	291
	clear exception log	293
	clear log	294
	clear log buffered	295
	clear log permanent	296
	connection-log events	297
	copy buffered-log	298
	copy permanent-log	299
	default log buffered	300
	default log console	301
	default log email	302
	default log host	303
	default log monitor	304
	default log permanent	305
	log buffered	306
	log buffered (filter)	307
	log buffered exclude	310
	log buffered size	313

	log console	314
	log console (filter)	315
	log console exclude	318
	log date-format	321
	log email	322
	log email (filter)	323
	log email exclude	326
	log email time	329
	log facility	331
	log host	333
	log host (filter)	335
	log host exclude	338
	log host source	341
	log host startup-delay	342
	log host time	344
	log monitor (filter)	346
	log monitor exclude	349
	log permanent	352
	log permanent (filter)	353
	log permanent exclude	356
	log permanent size	359
	log-rate-limit nsm	360
	log trustpoint	361
	log url-requests	362
	show connection-log events	363
	show counter log	364
	show exception log	365
	show log	366
	show log config	368
	show log permanent	370
	show running-config log	372
Chapter 10:	Scripting Commands	373
	Introduction	373
	activate	374
	echo	375
	wait	376
Chapter 11:	Interface Commands	377
	Introduction	377
	description (interface)	378
	interface (to configure)	379
	ip tcp adjust-mss	381
	ipv6 tcp adjust-mss	383
	mtu	385
	service statistics interfaces counter	387
	show interface	388
	show interface brief	391
	show interface status	392
	shutdown	394
PART 2:	Interfaces and Layer 2	395

Chapter 12:	Bridging Commands	396
	Introduction	396
	ageing-time	397
	bridge	398
	bridge-group	399
	l3-filtering enable	401
	mac-learning	402
	show bridge	403
	show bridge macaddr	405
Chapter 13:	802.1Q Encapsulation Commands	406
	Introduction	406
	encapsulation dot1q	407
Chapter 14:	PPP Commands	409
	Introduction	409
	debug ppp	411
	encapsulation ppp	414
	interface (PPP)	415
	ip address negotiated	416
	ip tcp adjust-mss	418
	ip unnumbered	420
	ipv6 tcp adjust-mss	422
	keepalive (PPP)	424
	mtu (PPP)	426
	peer default ip address	427
	peer neighbor-route	429
	ppp authentication	431
	ppp authentication refuse	433
	ppp hostname	435
	ppp ipcp dns	437
	ppp ipcp dns suffix-list	439
	ppp ipcp ip-override	441
	ppp password	442
	ppp service-name (PPPoE)	443
	ppp timeout idle	444
	ppp username	445
	show debugging ppp	446
	show interface (PPP)	447
	undebg ppp	451
Chapter 15:	PPP over Ethernet (PPPoE) Commands	452
	Introduction	452
	client (pppoe-relay)	453
	max-sessions	454
	pppoe-relay	455
	server (pppoe-relay)	456
	show running-config pppoe-relay	457
	timeout (pppoe-relay)	458
PART 3:	Routing	459

Chapter 16:	IP Addressing and Protocol Commands	460
	Introduction	460
	arp	462
	arp log	463
	arp opportunistic-nd	466
	arp-loose-check	467
	arp-reply-bc-dmac	469
	clear arp-cache	470
	debug ip packet interface	471
	ip address (IP Addressing and Protocol)	473
	ip directed-broadcast	475
	ip forwarding	477
	ip forward-protocol udp	478
	ip helper-address	480
	ip icmp error-interval	482
	ip icmp-timestamp	483
	ip limited-local-proxy-arp	484
	ip local-proxy-arp	485
	ip proxy-arp	486
	ip redirects	487
	ip tcp synack-retries	488
	ip tcp timeout established	489
	ip tcp-timestamp	490
	ip unreachable	491
	local-proxy-arp	493
	ping	494
	show arp	495
	show debugging ip packet	497
	show ip flooding-nexthops	498
	show ip forwarding	499
	show ip interface	500
	show ip sockets	501
	show ip traffic	504
	tcpdump	506
	traceroute	507
	undebg ip packet interface	508
 Chapter 17:	 Domain Name Service (DNS) Commands	 509
	Introduction	509
	accept-invalid-sslcert	512
	clear ip dns forwarding cache	513
	custom-failure	514
	custom-success	515
	ddns enable	516
	ddns-update-method	517
	ddns-update now	519
	debug ddns	520
	debug ip dns forwarding	521
	description (domain-list)	522
	domain	523
	expect-html-response	524
	follow-redirects	525

get-before-submit	526
get-params	527
host-name (ddns-update-method)	528
ip ddns-update-method	529
ip dns forwarding	530
ip dns forwarding cache	531
ip dns forwarding dead-time	532
ip dns forwarding domain-list	533
ip dns forwarding retry	534
ip dns forwarding source-interface	535
ip dns forwarding timeout	536
ip domain-list	537
ip domain-lookup	538
ip domain-name	540
ip name-server	541
ip name-server preferred-order	543
ipv6 ddns-update-method	544
obey-form	545
password (ddns-update-method)	546
ppp ipcp dns	547
ppp ipcp dns suffix-list	549
retry-interval	551
show ddns-update-method status	552
show debugging ip dns forwarding	553
show hosts	554
show ip dns forwarding	555
show ip dns forwarding cache	556
show ip dns forwarding server	557
show ip domain-list	558
show ip domain-name	559
show ip name-server	560
suppress-ipv4-updates	561
undebug ddns	562
update-interval (ddns-update-method)	563
update-url (ddns-update-method)	564
use-ipv4-for-ipv6-updates	567
username (ddns-update-method)	568

Chapter 18: IPv6 Commands 569

Introduction	569
clear ipv6 neighbors	571
ipv6 address	572
ipv6 address autoconfig	574
ipv6 address suffix	576
ipv6 enable	577
ipv6 eui64-linklocal	579
ipv6 forwarding	580
ipv6 icmp error-interval	581
ipv6 multicast forward-slow-path-packet	582
ipv6 multihoming	583
ipv6 nd accept-ra-default-routes	584
ipv6 nd accept-ra-pinfo	585
ipv6 nd current-hoplimit	586

ipv6 nd dns search-list	588
ipv6 nd dns-server	589
ipv6 nd managed-config-flag	591
ipv6 nd minimum-ra-interval	592
ipv6 nd other-config-flag	594
ipv6 nd prefix	595
ipv6 nd proxy interface	597
ipv6 nd ra-interval	598
ipv6 nd ra-lifetime	599
ipv6 nd reachable-time	601
ipv6 nd retransmission-time	603
ipv6 nd route-information	605
ipv6 nd router-preference	606
ipv6 nd suppress-ra	607
ipv6 opportunistic-nd	608
ipv6 route	609
ipv6 unreachable	611
ping ipv6	612
show ipv6 forwarding	614
show ipv6 interface	615
show ipv6 neighbors	616
show ipv6 route	617
show ipv6 route summary	619
traceroute ipv6	620

Chapter 19: Routing Commands 621

Introduction	621
ip resolve-via-default	622
ip route	623
ipv6 route	626
max-fib-routes	628
max-static-routes	629
maximum-paths	630
show ip resolve-via-default	631
show ip route	632
show ip route database	635
show ip route summary	637
show ipv6 route	638
show ipv6 route summary	640

Chapter 20: RIP Commands 641

Introduction	641
accept-lifetime	643
alliedware-behavior	645
cisco-metric-behavior (RIP)	647
clear ip rip route	648
debug rip	649
default-information originate (RIP)	650
default-metric (RIP)	651
distance (RIP)	652
distribute-list (RIP)	653
fullupdate (RIP)	654

ip summary-address rip	655
ip prefix-list	656
ip rip authentication key-chain	658
ip rip authentication mode	660
ip rip authentication string	662
ip rip receive-packet	664
ip rip receive version	665
ip rip send-packet	666
ip rip send version	667
ip rip send version 1-compatible	669
ip rip split-horizon	670
key	671
key chain	672
key-string	673
maximum-prefix	674
neighbor (RIP)	675
network (RIP)	676
passive-interface (RIP)	677
recv-buffer-size (RIP)	678
redistribute (RIP)	679
restart rip graceful	680
rip restart grace-period	681
route (RIP)	682
router rip	683
send-lifetime	684
show debugging rip	686
show ip prefix-list	687
show ip protocols rip	688
show ip rip	689
show ip rip database	690
show ip rip interface	691
timers (RIP)	692
undebg rip	694
version (RIP)	695

Chapter 21: RIPng for IPv6 Commands 696

Introduction	696
aggregate-address (IPv6 RIPng)	698
clear ipv6 rip route	699
debug ipv6 rip	700
default-information originate (IPv6 RIPng)	701
default-metric (IPv6 RIPng)	702
distribute-list (IPv6 RIPng)	703
ipv6 prefix-list	704
ipv6 rip metric-offset	706
ipv6 rip split-horizon	708
ipv6 router rip	709
neighbor (IPv6 RIPng)	710
passive-interface (IPv6 RIPng)	711
recv-buffer-size (IPv6 RIPng)	712
redistribute (IPv6 RIPng)	713
route (IPv6 RIPng)	714
router ipv6 rip	715

show debugging ipv6 rip	716
show ipv6 prefix-list	717
show ipv6 protocols rip	718
show ipv6 rip	719
show ipv6 rip database	720
show ipv6 rip interface	721
timers (IPv6 RIPng)	722
undebg ipv6 rip	723

Chapter 22:

OSPF Commands	724
Introduction	724
area default-cost	727
area authentication	728
area filter-list	729
area nssa	730
area range	732
area stub	734
area virtual-link	735
auto-cost reference bandwidth	738
bandwidth	740
capability opaque	741
capability restart	742
clear ip ospf process	743
compatible rfc1583	744
debug ospf events	745
debug ospf ifsm	746
debug ospf lsa	747
debug ospf nfsm	748
debug ospf nsm	749
debug ospf packet	750
debug ospf route	751
default-information originate	752
default-metric (OSPF)	753
distance (OSPF)	754
distribute-list (OSPF)	756
enable db-summary-opt	758
host area	759
ip ospf authentication	760
ip ospf authentication-key	761
ip ospf cost	762
ip ospf database-filter	763
ip ospf dead-interval	764
ip ospf disable all	765
ip ospf hello-interval	766
ip ospf message-digest-key	767
ip ospf mtu	769
ip ospf mtu-ignore	770
ip ospf network	771
ip ospf priority	772
ip ospf resync-timeout	773
ip ospf retransmit-interval	774
ip ospf transmit-delay	775
max-concurrent-dd	776

maximum-area	777
neighbor (OSPF)	778
network area	779
ospf abr-type	781
ospf restart grace-period	782
ospf restart helper	783
ospf router-id	785
overflow database	786
overflow database external	787
passive-interface (OSPF)	788
redistribute (OSPF)	789
restart ospf graceful	791
router ospf	792
router-id	793
show debugging ospf	794
show ip ospf	795
show ip ospf border-routers	798
show ip ospf database	799
show ip ospf database asbr-summary	801
show ip ospf database external	802
show ip ospf database network	804
show ip ospf database nssa-external	805
show ip ospf database opaque-area	807
show ip ospf database opaque-as	808
show ip ospf database opaque-link	809
show ip ospf database router	810
show ip ospf database summary	812
show ip ospf interface	815
show ip ospf neighbor	816
show ip ospf route	818
show ip ospf virtual-links	819
show ip protocols ospf	820
summary-address	821
timers spf exp	822
undebg ospf events	823
undebg ospf ifsm	824
undebg ospf lsa	825
undebg ospf n fsm	826
undebg ospf nsm	827
undebg ospf packet	828
undebg ospf route	829

Chapter 23:	OSPFv3 for IPv6 Commands	830
	Introduction	830
	abr-type	833
	area authentication ipsec spi	834
	area default-cost (IPv6 OSPF)	836
	area encryption ipsec spi esp	837
	area range (IPv6 OSPF)	840
	area stub (IPv6 OSPF)	842
	area virtual-link (IPv6 OSPF)	843
	area virtual-link authentication ipsec spi	845
	area virtual-link encryption ipsec spi	847

auto-cost reference bandwidth (IPv6 OSPF)	850
bandwidth	852
clear ipv6 ospf process	853
debug ipv6 ospf events	854
debug ipv6 ospf ifsm	855
debug ipv6 ospf lsa	856
debug ipv6 ospf nfsm	857
debug ipv6 ospf packet	858
debug ipv6 ospf route	859
default-information originate	860
default-metric (IPv6 OSPF)	861
distance (IPv6 OSPF)	862
ipv6 ospf authentication spi	864
ipv6 ospf cost	866
ipv6 ospf dead-interval	867
ipv6 ospf display route single-line	868
ipv6 ospf encryption spi esp	869
ipv6 ospf hello-interval	872
ipv6 ospf neighbor	873
ipv6 ospf network	875
ipv6 ospf priority	876
ipv6 ospf retransmit-interval	877
ipv6 ospf transmit-delay	878
ipv6 router ospf area	879
max-concurrent-dd (IPv6 OSPF)	881
passive-interface (IPv6 OSPF)	882
redistribute (IPv6 OSPF)	883
restart ipv6 ospf graceful	885
router ipv6 ospf	886
router-id (IPv6 OSPF)	887
show debugging ipv6 ospf	888
show ipv6 ospf	889
show ipv6 ospf database	891
show ipv6 ospf database external	892
show ipv6 ospf database grace	893
show ipv6 ospf database inter-prefix	894
show ipv6 ospf database inter-router	895
show ipv6 ospf database intra-prefix	896
show ipv6 ospf database link	897
show ipv6 ospf database network	898
show ipv6 ospf database router	900
show ipv6 ospf interface	905
show ipv6 ospf neighbor	906
show ipv6 ospf route	907
show ipv6 ospf virtual-links	908
summary-address (IPv6 OSPF)	909
timers spf exp (IPv6 OSPF)	911
undebug ipv6 ospf events	912
undebug ipv6 ospf ifsm	913
undebug ipv6 ospf lsa	914
undebug ipv6 ospf nfsm	915
undebug ipv6 ospf packet	916
undebug ipv6 ospf route	917

Chapter 24:

BGP and BGP4+ Commands	918
Introduction	918
address-family	924
aggregate-address	926
auto-summary (BGP only)	929
bgp aggregate-nexthop-check	931
bgp always-compare-med	932
bgp bestpath as-path ignore	934
bgp bestpath compare-confed-aspath	935
bgp bestpath compare-routerid	936
bgp bestpath med	937
bgp bestpath med remove-recv-med	939
bgp bestpath med remove-send-med	940
bgp client-to-client reflection	941
bgp cluster-id	942
bgp confederation identifier	944
bgp confederation peers	945
bgp config-type	947
bgp dampening	949
bgp damp-peer-oscillation (BGP only)	951
bgp default ipv4-unicast	952
bgp default local-preference (BGP only)	953
bgp deterministic-med	954
bgp enforce-first-as	956
bgp fast-external-failover	957
bgp graceful-restart	958
bgp graceful-restart graceful-reset	960
bgp log-neighbor-changes	961
bgp memory maxallocation	963
bgp nexthop-trigger-count	964
bgp nexthop-trigger delay	965
bgp nexthop-trigger enable	966
bgp rfc1771-path-select (BGP only)	967
bgp rfc1771-strict (BGP only)	968
bgp router-id	969
bgp scan-time (BGP only)	971
bgp update-delay	972
clear bgp *	973
clear bgp (IPv4 or IPv6 address)	974
clear bgp (ASN)	976
clear bgp external	977
clear bgp peer-group	978
clear bgp ipv6 (ipv6 address) (BGP4+ only)	979
clear bgp ipv6 dampening (BGP4+ only)	980
clear bgp ipv6 flap-statistics (BGP4+ only)	981
clear bgp ipv6 (ASN) (BGP4+ only)	982
clear bgp ipv6 external (BGP4+ only)	983
clear bgp ipv6 peer-group (BGP4+ only)	984
clear ip bgp * (BGP only)	985
clear ip bgp (IPv4) (BGP only)	986
clear ip bgp dampening (BGP only)	987
clear ip bgp flap-statistics (BGP only)	988
clear ip bgp (ASN) (BGP only)	989

clear ip bgp external (BGP only)	990
clear ip bgp peer-group (BGP only)	991
clear ip prefix-list	992
debug bgp (BGP only)	993
distance (BGP and BGP4+)	995
exit-address-family	997
ip community-list	998
ip community-list expanded	1000
ip community-list standard	1002
ip extcommunity-list expanded	1004
ip extcommunity-list standard	1006
ip prefix-list	1008
ipv6 prefix-list	1010
match as-path	1012
match community	1013
max-paths	1015
neighbor activate	1016
neighbor advertisement-interval	1019
neighbor allowas-in	1022
neighbor as-origination-interval	1025
neighbor attribute-unchanged	1027
neighbor capability graceful-restart	1030
neighbor capability orf prefix-list	1033
neighbor capability route-refresh	1036
neighbor collide-established	1039
neighbor default-originate	1042
neighbor description	1045
neighbor disallow-infinite-holdtime	1048
neighbor dont-capability-negotiate	1050
neighbor ebgp-multihop	1053
neighbor enforce-multihop	1056
neighbor filter-list	1059
neighbor interface	1062
neighbor local-as	1064
neighbor maximum-prefix	1067
neighbor next-hop-self	1070
neighbor override-capability	1073
neighbor passive	1075
neighbor password	1078
neighbor peer-group (add a neighbor)	1081
neighbor peer-group (create a peer-group)	1083
neighbor port	1084
neighbor prefix-list	1087
neighbor remote-as	1090
neighbor remove-private-AS (BGP only)	1093
neighbor restart-time	1095
neighbor route-map	1098
neighbor route-reflector-client (BGP only)	1102
neighbor route-server-client (BGP only)	1104
neighbor send-community	1105
neighbor shutdown	1109
neighbor soft-reconfiguration inbound	1111
neighbor timers	1114

neighbor transparent-as	1117
neighbor transparent-nexthop	1119
neighbor unsuppress-map	1121
neighbor update-source	1124
neighbor version (BGP only)	1128
neighbor weight	1130
network (BGP and BGP4+)	1133
network synchronization	1136
redistribute (into BGP or BGP4+)	1137
restart bgp graceful (BGP only)	1139
router bgp	1140
route-map	1141
set as-path	1144
set community	1145
show bgp ipv6 (BGP4+ only)	1147
show bgp ipv6 community (BGP4+ only)	1148
show bgp ipv6 community-list (BGP4+ only)	1150
show bgp ipv6 dampening (BGP4+ only)	1151
show bgp ipv6 filter-list (BGP4+ only)	1152
show bgp ipv6 inconsistent-as (BGP4+ only)	1153
show bgp ipv6 longer-prefixes (BGP4+ only)	1154
show bgp ipv6 neighbors (BGP4+ only)	1155
show bgp ipv6 paths (BGP4+ only)	1158
show bgp ipv6 prefix-list (BGP4+ only)	1159
show bgp ipv6 quote-regexp (BGP4+ only)	1160
show bgp ipv6 regexp (BGP4+ only)	1161
show bgp ipv6 route-map (BGP4+ only)	1163
show bgp ipv6 summary (BGP4+ only)	1164
show bgp memory maxallocation (BGP only)	1165
show bgp nexthop-tracking (BGP only)	1166
show bgp nexthop-tree-details (BGP only)	1167
show debugging bgp (BGP only)	1168
show ip bgp (BGP only)	1169
show ip bgp attribute-info (BGP only)	1170
show ip bgp cidr-only (BGP only)	1171
show ip bgp community (BGP only)	1172
show ip bgp community-info (BGP only)	1174
show ip bgp community-list (BGP only)	1175
show ip bgp dampening (BGP only)	1176
show ip bgp filter-list (BGP only)	1178
show ip bgp inconsistent-as (BGP only)	1179
show ip bgp longer-prefixes (BGP only)	1180
show ip bgp neighbors (BGP only)	1181
show ip bgp neighbors connection-retrytime (BGP only)	1184
show ip bgp neighbors hold-time (BGP only)	1185
show ip bgp neighbors keepalive (BGP only)	1186
show ip bgp neighbors keepalive-interval (BGP only)	1187
show ip bgp neighbors notification (BGP only)	1188
show ip bgp neighbors open (BGP only)	1189
show ip bgp neighbors rcvd-msgs (BGP only)	1190
show ip bgp neighbors sent-msgs (BGP only)	1191
show ip bgp neighbors update (BGP only)	1192
show ip bgp paths (BGP only)	1193

show ip bgp prefix-list (BGP only)	1194
show ip bgp quote-regexp (BGP only)	1195
show ip bgp regexp (BGP only)	1197
show ip bgp route-map (BGP only)	1199
show ip bgp scan (BGP only)	1200
show ip bgp summary (BGP only)	1201
show ip community-list	1202
show ip extcommunity-list	1203
show ip prefix-list	1204
show ipv6 prefix-list	1205
show ip protocols bgp (BGP only)	1206
show route-map	1207
synchronization	1208
timers (BGP)	1210
undebg bgp (BGP only)	1212

Chapter 25: Route Map Commands 1213

Introduction	1213
match as-path	1215
match community	1216
match interface	1218
match ip address	1219
match ip next-hop	1221
match ipv6 address	1223
match ipv6 next-hop	1225
match metric	1226
match origin	1227
match route-type	1229
match tag	1230
route-map	1231
set aggregator	1234
set as-path	1235
set atomic-aggregate	1236
set comm-list delete	1237
set community	1238
set dampening	1240
set extcommunity	1242
set ip next-hop (route map)	1244
set ipv6 next-hop	1245
set local-preference	1246
set metric	1247
set metric-type	1249
set origin	1250
set originator-id	1251
set tag	1252
set weight	1253
show route-map	1254

Chapter 26: Policy-based Routing Commands 1255

Introduction	1255
application-decision	1256
debug policy-based-routing	1258

	ip policy-route	1259
	ipv6 policy-route	1261
	policy-based-routing	1263
	policy-based-routing enable	1264
	show ip pbr route	1265
	show ipv6 pbr route	1267
	show pbr rules	1269
	show pbr rules brief	1274
Chapter 27:	SD-WAN Commands	1276
	Introduction	1276
	application-decision	1278
	consecutive probe loss	1280
	debug linkmon	1282
	destination (linkmon-probe)	1284
	dscp (linkmon-probe)	1286
	egress interface (linkmon-probe)	1287
	enable (linkmon-probe)	1288
	interval (linkmon-probe)	1289
	ip policy-route	1290
	ip-version (linkmon-probe)	1292
	ipv6 policy-route	1293
	jitter	1295
	latency	1297
	linkmon group	1299
	linkmon probe-history	1300
	linkmon probe	1302
	linkmon profile	1304
	load-balancing	1305
	member (linkmon-group)	1306
	pktloss	1308
	preference	1310
	sample-size (linkmon-probe)	1312
	show debugging linkmon	1313
	show linkmon probe	1314
	show linkmon probe-history	1317
	show pbr rules	1319
	show pbr rules brief	1324
	size (linkmon-probe)	1326
	source (linkmon-probe)	1327
	url (linkmon-probe)	1328
PART 4:	Multicast Applications	1329
Chapter 28:	IGMP Commands	1330
	Introduction	1330
	clear ip igmp	1332
	clear ip igmp group	1333
	clear ip igmp interface	1334
	debug igmp	1335
	ip igmp	1336
	ip igmp last-member-query-count	1337

ip igmp last-member-query-interval	1338
ip igmp mroute-proxy	1339
ip igmp proxy-service	1340
ip igmp querier-timeout	1341
ip igmp query-holdtime	1342
ip igmp query-interval	1344
ip igmp query-max-response-time	1346
ip igmp ra-option	1348
ip igmp robustness-variable	1349
ip igmp source-address-check	1350
ip igmp startup-query-count	1351
ip igmp startup-query-interval	1352
ip igmp version	1353
show debugging igmp	1354
show ip igmp groups	1355
show ip igmp interface	1357
undebug igmp	1359

Chapter 29: MLD Commands 1360

Introduction	1360
clear ipv6 mld	1362
clear ipv6 mld group	1363
clear ipv6 mld interface	1364
debug mld	1365
ipv6 mld	1366
ipv6 mld last-member-query-count	1367
ipv6 mld last-member-query-interval	1368
ipv6 mld querier-timeout	1369
ipv6 mld query-interval	1370
ipv6 mld query-max-response-time	1371
ipv6 mld robustness-variable	1372
ipv6 mld static-group	1373
ipv6 mld version	1374
show debugging mld	1375
show ipv6 mld groups	1376
show ipv6 mld interface	1378

Chapter 30: Multicast Commands 1379

Introduction	1379
clear ip mroute	1381
clear ip mroute statistics	1383
clear ip multicast route	1384
clear ipv6 mroute	1385
clear ipv6 mroute statistics	1386
debug nsm	1387
debug nsm mcast	1388
debug nsm mcast6	1389
ip mroute	1390
ip multicast handle-igmp-immediately	1392
ip multicast route	1393
ip multicast route-limit	1395
ip multicast wrong-vif-suppression	1396

ip multicast-routing	1397
ipv6 mroute	1398
ipv6 multicast route	1400
ipv6 multicast route-limit	1402
ipv6 multicast-routing	1403
show debugging nsm mcast	1404
show ip mroute	1405
show ip mvif	1408
show ip rpf	1409
show ipv6 mif	1410
show ipv6 mroute	1411
show ipv6 multicast forwarding	1413

Chapter 31:

PIM-SM Commands	1414
Introduction	1414
clear ip pim sparse-mode bsr rp-set *	1416
clear ip pim sparse-mode packet statistics	1417
clear ip mroute pim sparse-mode	1418
debug pim sparse-mode	1419
debug pim sparse-mode timer	1420
ip pim anycast-rp	1422
ip pim bsr-border	1423
ip pim bsr-candidate	1424
ip pim cisco-register-checksum	1425
ip pim crp-cisco-prefix	1426
ip pim dr-priority	1427
ip pim exclude-genid	1428
ip pim ext-srcs-directly-connected	1429
ip pim hello-holdtime (PIM-SM)	1430
ip pim hello-interval (PIM-SM)	1431
ip pim ignore-rp-set-priority	1432
ip pim jp-timer	1433
ip pim register-rate-limit	1434
ip pim register-rp-reachability	1435
ip pim register-source	1436
ip pim register-suppression	1437
ip pim rp-address	1438
ip pim rp-candidate	1440
ip pim rp-register-kat	1441
ip pim sparse-mode	1442
ip pim sparse-mode join-prune-batching	1443
ip pim sparse-mode passive	1444
ip pim sparse-mode wrong-vif-suppression	1445
ip pim spt-threshold	1446
ip pim ssm	1447
service pim	1448
show debugging pim sparse-mode	1449
show ip pim sparse-mode bsr-router	1450
show ip pim sparse-mode interface	1451
show ip pim sparse-mode interface detail	1453
show ip pim sparse-mode local-members	1454
show ip pim sparse-mode mroute	1455
show ip pim sparse-mode mroute detail	1457

show ip pim sparse-mode neighbor	1459
show ip pim sparse-mode nexthop	1461
show ip pim sparse-mode packet statistics	1462
show ip pim sparse-mode rp-hash	1463
show ip pim sparse-mode rp mapping	1464
undebg all pim sparse-mode	1465

Chapter 32:

PIM-SMv6 Commands	1466
Introduction	1466
clear ipv6 mroute pim	1469
clear ipv6 mroute pim sparse-mode	1470
clear ipv6 pim sparse-mode bsr rp-set *	1471
debug ipv6 pim sparse-mode	1472
debug ipv6 pim sparse-mode packet	1474
debug ipv6 pim sparse-mode timer	1475
ipv6 pim anycast-rp	1477
ipv6 pim bsr-border	1479
ipv6 pim bsr-candidate	1481
ipv6 pim cisco-register-checksum	1483
ipv6 pim crp-cisco-prefix	1484
ipv6 pim dr-priority	1485
ipv6 pim exclude-genid	1487
ipv6 pim ext-srcs-directly-connected	1488
ipv6 pim hello-holdtime	1489
ipv6 pim hello-interval	1491
ipv6 pim ignore-rp-set-priority	1492
ipv6 pim jp-timer	1493
ipv6 pim register-rate-limit	1494
ipv6 pim register-rp-reachability	1495
ipv6 pim register-source	1496
ipv6 pim register-suppression	1498
ipv6 pim rp-address	1499
ipv6 pim rp-candidate	1500
ipv6 pim rp embedded	1501
ipv6 pim rp-register-kat	1502
ipv6 pim sparse-mode	1503
ipv6 pim sparse-mode passive	1504
ipv6 pim spt-threshold	1505
ipv6 pim ssm	1506
ipv6 pim unicast-bsm	1507
service pim6	1508
show debugging ipv6 pim sparse-mode	1509
show ipv6 pim sparse-mode bsr-router	1510
show ipv6 pim sparse-mode interface	1511
show ipv6 pim sparse-mode interface detail	1513
show ipv6 pim sparse-mode local-members	1514
show ipv6 pim sparse-mode mroute	1515
show ipv6 pim sparse-mode mroute detail	1517
show ipv6 pim sparse-mode neighbor	1519
show ipv6 pim sparse-mode nexthop	1520
show ipv6 pim sparse-mode rp-hash	1522
show ipv6 pim sparse-mode rp mapping	1523
show ipv6 pim sparse-mode rp nexthop	1524

	undebg all ipv6 pim sparse-mode	1526
	undebg ipv6 pim sparse-mode	1527
PART 5:	Access and Security	1529
Chapter 33:	Traffic Control Commands	1530
	Introduction	1530
	class (htb)	1532
	class (priority)	1534
	class (wrr)	1536
	debug traffic-control	1538
	interface (traffic-control)	1539
	interface dynamic-virtual-bandwidth	1541
	l3-filtering enable	1543
	move rule (traffic-control)	1544
	policy (traffic-control)	1545
	red-curve	1547
	rule (traffic-control)	1549
	show debugging traffic-control	1551
	show running-config traffic-control	1552
	show traffic-control counters	1553
	show traffic-control interface	1555
	show traffic-control policy	1556
	show traffic-control red-curve	1558
	show traffic-control rule config-check	1560
	show traffic-control rule	1561
	show traffic-control	1562
	sub-class (htb)	1563
	sub-class (priority)	1565
	sub-class (wrr)	1567
	sub-sub-class (htb)	1569
	sub-sub-class (priority)	1571
	sub-sub-class (wrr)	1573
	traffic-control enable	1575
	traffic-control	1576
Chapter 34:	AAA Commands	1578
	Introduction	1578
	aaa accounting commands	1580
	aaa accounting login	1582
	aaa accounting openvpn	1585
	aaa accounting update	1587
	aaa authentication 2fa-registration default group	1589
	aaa authentication download-portal	1591
	aaa authentication enable default group tacacs+	1593
	aaa authentication enable default local	1595
	aaa authentication isakmp	1596
	aaa authentication login	1597
	aaa authentication openvpn	1600
	aaa authorization commands	1602
	aaa authorization config-commands	1604
	aaa group server	1605

aaa local authentication attempts logout-time	1607
aaa local authentication attempts max-fail	1608
aaa local authentication attempts max-fail remote-login-only	1609
aaa login fail-delay	1610
accounting login	1611
authorization commands	1612
clear aaa local user logout	1614
debug aaa	1615
login authentication	1616
proxy-port	1617
radius-secure-proxy aaa	1618
server (radsecproxy-aaa)	1619
server mutual-authentication	1621
server name-check	1622
server trustpoint	1623
show aaa local user locked	1625
show aaa server group	1627
show debugging aaa	1628
show radius server group	1629
undebug aaa	1631

Chapter 35: Lightweight Directory Access Protocol (LDAP) Commands 1632

Introduction	1632
authentication (ldap-server)	1634
base-dn	1636
bind authenticate root-dn	1637
deadtime (ldap-server)	1638
debug ldap client	1639
group-attribute	1641
group-dn	1642
host (ldap-server)	1643
ldap-server	1645
login-attribute	1647
port (ldap-server)	1649
retransmit (ldap-server)	1650
search-filter	1651
secure cipher (ldap-server)	1653
secure mode (ldap-server)	1655
secure trustpoint (ldap-server)	1657
server (ldap-group)	1658
show ldap server group	1659
timeout (ldap-server)	1661

Chapter 36: RADIUS Commands 1662

Introduction	1662
auth-mac-promiscuous	1663
deadtime (RADIUS server group)	1664
debug radius	1665
ip radius require-message-authenticator	1666
ip radius source-interface	1667
radius-server deadtime	1668
radius-server host	1669

radius-server key	1672
radius-server retransmit	1673
radius-server timeout	1675
server (RADIUS server group)	1677
show debugging radius	1679
show radius	1680
show radius local-server auth-mac-promiscuous	1683
undebg radius	1684

Chapter 37: Local RADIUS Server Commands 1685

Introduction	1685
attribute (radsrv-grp)	1687
authentication	1689
client (radsecproxy-srv)	1690
client mutual-authentication	1692
client name-check	1693
client trustpoint	1694
clear radius local-server statistics	1695
copy fdb-radius-users (to file)	1696
copy local-radius-user-db (from file)	1698
copy local-radius-user-db (to file)	1699
crypto pki enroll local (deleted)	1700
crypto pki enroll local local-radius-all-users (deleted)	1701
crypto pki enroll local user (deleted)	1702
crypto pki export local pem (deleted)	1703
crypto pki export local pkcs12 (deleted)	1704
crypto pki trustpoint local (deleted)	1705
debug crypto pki (deleted)	1706
domain-style	1707
egress-vlan-id (radsrv-grp)	1708
egress-vlan-name (radsrv-grp)	1709
group (radsrv)	1710
help radius-attribute	1711
nas	1713
nas message-authenticator (radsrv)	1714
radius-secure-proxy local-server	1716
radius-server local	1717
server auth-port	1718
server enable	1719
server trustpoint (radsrv)	1720
show radius local-server group	1722
show radius local-server nas	1723
show radius local-server statistics	1724
show radius local-server trustpoint	1726
show radius local-server user	1727
user (radsrv)	1729
vlan (radsrv-grp)	1731

Chapter 38: Two-factor Authentication (2FA) Commands 1732

Introduction	1732
2fa allow-reuse	1734
2fa create user	1735

2fa create user email	1737
2fa create user skip-2fa	1738
2fa delete user	1739
2fa email-expiry-time	1740
2fa email-otp	1741
2fa email-template	1742
2fa export user-data	1744
2fa hotp-window-size	1745
2fa import user-data source	1746
2fa issuer	1748
2fa label	1750
2fa max-skew	1752
2fa radius-email-attribute	1753
2fa reject-unconfigured-users	1755
2fa reset scratch-codes	1756
2fa reset skew	1757
2fa skew adjust	1758
2fa totp-window-size	1760
2fa self-registration port	1761
aaa authentication 2fa-registration default group	1763
debug 2fa	1765
email-attribute (ldap-server)	1766
service 2fa	1767
show 2fa	1769
show 2fa email-template	1770
show 2fa user	1771
show 2fa users	1773
show debugging 2fa	1774
undebug 2fa	1775

Chapter 39: Public Key Infrastructure and Crypto Commands 1776

Introduction	1776
crypto key generate rsa	1778
crypto key zeroize	1779
crypto pki authenticate	1780
crypto pki enroll	1781
crypto pki enroll user	1782
crypto pki export pem	1784
crypto pki export pkcs12	1785
crypto pki import pem	1787
crypto pki import pkcs12	1789
crypto pki trustpoint	1790
enrollment (ca-trustpoint)	1791
fingerprint (ca-trustpoint)	1792
no crypto pki certificate	1794
rsakeypair (ca-trustpoint)	1795
show crypto key mypubkey rsa	1796
show crypto pki certificates	1797
show crypto pki enrollment user	1799
show crypto pki trustpoint	1800
show hash	1801
subject-name (ca-trustpoint)	1802

Chapter 40:	TACACS+ Commands	1804
	Introduction	1804
	aaa authorization commands	1805
	aaa authorization config-commands	1807
	authorization commands	1808
	ip tacacs source-interface	1810
	show tacacs+	1811
	tacacs-server host	1813
	tacacs-server key	1815
	tacacs-server timeout	1816
PART 6:	High Availability	1817
Chapter 41:	VRRP Commands	1818
	Introduction	1818
	advertisement-interval	1820
	alternate-checksum-mode	1822
	circuit-failover	1823
	debug vrrp	1825
	debug vrrp events	1826
	debug vrrp packet	1827
	disable (VRRP)	1828
	enable (VRRP)	1829
	preempt-mode	1830
	priority	1832
	router ipv6 vrrp (interface)	1834
	router vrrp (interface)	1836
	show debugging vrrp	1838
	show running-config router ipv6 vrrp	1839
	show running-config router vrrp	1840
	show vrrp	1841
	show vrrp counters	1843
	show vrrp ipv6	1846
	show vrrp (session)	1847
	transition-mode	1848
	undebg vrrp	1850
	undebg vrrp events	1851
	undebg vrrp packet	1852
	virtual-ip	1853
	virtual-ipv6	1855
	vrrp vmac	1857
PART 7:	Network Management	1858
Chapter 42:	AMF and AMF Plus Commands	1859
	Introduction	1859
	application-proxy ip-filter	1865
	application-proxy quarantine-vlan	1866
	application-proxy redirect-url	1867
	application-proxy threat-protection	1868
	application-proxy threat-protection send-summary	1870
	application-proxy whitelist advertised-address	1871

application-proxy whitelist enable	1872
application-proxy whitelist protection tls	1873
application-proxy whitelist server	1874
application-proxy whitelist trustpoint (deprecated)	1876
area-link	1877
atmf-arealink	1879
atmf-link	1881
atmf amfplus-license-only	1882
atmf area	1884
atmf area password	1886
atmf authorize	1888
atmf authorize provision	1890
atmf backup	1892
atmf backup area-masters delete	1893
atmf backup area-masters enable	1894
atmf backup area-masters now	1895
atmf backup area-masters synchronize	1896
atmf backup bandwidth	1897
atmf backup delete	1898
atmf backup enable	1899
atmf backup guests delete	1900
atmf backup guests enable	1901
atmf backup guests now	1902
atmf backup guests synchronize	1903
atmf backup now	1904
atmf backup redundancy enable	1906
atmf backup server	1907
atmf backup stop	1909
atmf backup synchronize	1910
atmf cleanup	1911
atmf container	1912
atmf container login	1913
atmf controller	1914
atmf distribute firmware	1915
atmf domain vlan	1917
atmf enable	1920
atmf group (membership)	1921
atmf guest-class	1923
atmf log-verbose	1925
atmf management subnet	1926
atmf management vlan	1929
atmf master	1931
atmf mtu	1932
atmf network-name	1933
atmf provision (interface)	1934
atmf provision node	1935
atmf reboot-rolling	1937
atmf recover	1941
atmf recover guest	1943
atmf recover led-off	1944
atmf recover over-eth	1945
atmf recovery-server	1946
atmf remote-login	1948

atmf restricted-login	1950
atmf retry guest-link	1952
atmf secure-mode	1953
atmf secure-mode certificate expire	1955
atmf secure-mode certificate expiry	1956
atmf secure-mode certificate renew	1957
atmf secure-mode enable-all	1958
atmf select-area	1960
atmf topology-gui enable	1961
atmf trustpoint	1962
atmf virtual-crosslink	1964
atmf virtual-link	1966
atmf virtual-link description	1969
atmf virtual-link protection	1970
atmf working-set	1972
bridge-group (amf-container)	1974
clear application-proxy threat-protection	1976
clear atmf links	1977
clear atmf links virtual	1978
clear atmf links statistics	1979
clear atmf recovery-file	1980
clear atmf secure-mode certificates	1981
clear atmf secure-mode statistics	1982
clone (amf-provision)	1983
configure boot config (amf-provision)	1985
configure boot system (amf-provision)	1987
copy (amf-provision)	1989
create (amf-provision)	1990
debug atmf	1992
debug atmf packet	1994
delete (amf-provision)	1997
discovery	1999
description (amf-container)	2001
erase factory-default	2002
firmware-url	2003
http-enable	2005
identity (amf-provision)	2007
license-cert (amf-provision)	2009
locate (amf-provision)	2011
log event-host	2013
login-fallback enable	2014
modeltype	2015
service atmf-application-proxy	2016
show application-proxy threat-protection	2017
show application-proxy whitelist advertised-address	2019
show application-proxy whitelist interface	2020
show application-proxy whitelist server	2022
show application-proxy whitelist supplicant	2023
show atmf	2025
show atmf area	2029
show atmf area guests	2032
show atmf area guests-detail	2034
show atmf area nodes	2036

show atmf area nodes-detail	2038
show atmf area summary	2040
show atmf authorization	2041
show atmf backup	2044
show atmf backup area	2048
show atmf backup guest	2050
show atmf container	2052
show atmf detail	2055
show atmf group	2057
show atmf group members	2059
show atmf guests	2061
show atmf guests detail	2063
show atmf links	2066
show atmf links detail	2068
show atmf links guest	2077
show atmf links guest detail	2079
show atmf links statistics	2083
show atmf nodes	2086
show atmf provision nodes	2088
show atmf recovery-file	2090
show atmf secure-mode	2091
show atmf secure-mode audit	2093
show atmf secure-mode audit link	2094
show atmf secure-mode certificates	2095
show atmf secure-mode sa	2098
show atmf secure-mode statistics	2101
show atmf tech	2103
show atmf virtual-links	2106
show atmf working-set	2108
show debugging atmf	2109
show debugging atmf packet	2110
show running-config atmf	2111
state	2112
switchport atmf-agentlink	2114
switchport atmf-arealink	2115
switchport atmf-crosslink	2117
switchport atmf-guestlink	2119
switchport atmf-link	2121
type atmf guest	2122
type atmf node	2123
undebg atmf	2125
username (atmf-guest)	2126

Chapter 43:	STOAT Commands	2127
	Introduction	2127
	clear stoat collector session counters	2129
	description (stoat-dest)	2130
	key (stoat-dest)	2131
	name-check (stoat-dest)	2132
	service stoat	2133
	show stoat collector	2134
	show stoat destinations	2136
	shutdown (stoat-dest)	2138

	stoat collector enable	2139
	stoat collector expiry-period	2140
	stoat collector key	2141
	stoat collector trustpoint	2143
	stoat destination	2144
	trustpoint (stoat-dest)	2146
	unique-id	2147
Chapter 44:	Device Discovery using SNMP Commands	2148
	Introduction	2148
	clear snmp-discovery	2149
	service snmp-discovery	2150
	show running-config snmp-discovery	2151
	show snmp-discovery	2152
	snmp-discovery arp-polling-interval	2154
	snmp-discovery community	2155
	snmp-discovery deny	2156
	snmp-discovery permit	2158
	snmp-discovery snmp-polling-interval	2159
	snmp-discovery snmp-version	2160
	snmp-discovery user	2161
Chapter 45:	Dynamic Host Configuration Protocol (DHCP) Commands	2163
	Introduction	2163
	bootfile	2165
	clear ip dhcp binding	2166
	default-router	2167
	dns-server	2168
	domain-name	2169
	host (DHCP)	2170
	ip address dhcp	2171
	ip dhcp bootp ignore	2173
	ip dhcp leasequery enable	2174
	ip dhcp option	2175
	ip dhcp pool	2177
	ip dhcp-client default-route distance	2178
	ip dhcp-client request vendor-identifying-specific	2180
	ip dhcp-client vendor-identifying-class	2181
	ip dhcp-relay agent-option	2182
	ip dhcp-relay agent-option checking	2184
	ip dhcp-relay agent-option remote-id	2185
	ip dhcp-relay information policy	2186
	ip dhcp-relay maxhops	2188
	ip dhcp-relay max-message-length	2189
	ip dhcp-relay server-address	2191
	ip dhcp-relay short-lease	2193
	ip dhcp-relay use-client-side-address	2194
	lease	2195
	network (DHCP)	2197
	next-server	2198
	option	2199
	probe enable	2201

probe packets	2202
probe timeout	2203
probe type	2204
range	2205
route	2206
service dhcp-relay	2207
service dhcp-server	2208
short-lease-threshold	2209
show counter dhcp-client	2211
show counter dhcp-relay	2212
show counter dhcp-server	2215
show dhcp lease	2217
show ip dhcp binding	2218
show ip dhcp pool	2220
show ip dhcp-relay	2225
show ip dhcp server statistics	2226
show ip dhcp server summary	2228
subnet-mask	2229

Chapter 46: DHCP for IPv6 (DHCPv6) Commands 2230

Introduction	2230
address prefix	2232
address range	2234
clear counter ipv6 dhcp-client	2236
clear counter ipv6 dhcp-server	2237
clear ipv6 dhcp binding	2238
clear ipv6 dhcp client	2240
dns-server (DHCPv6)	2241
domain-name (DHCPv6)	2243
ip dhcp-relay agent-option	2244
ip dhcp-relay agent-option checking	2246
ip dhcp-relay agent-option remote-id	2247
ip dhcp-relay information policy	2248
ip dhcp-relay maxhops	2250
ip dhcp-relay max-message-length	2251
ip dhcp-relay server-address	2253
ip dhcp-relay short-lease-ipv6	2255
ipv6 address (DHCPv6 PD)	2256
ipv6 address dhcp	2258
ipv6 dhcp client pd	2260
ipv6 dhcp option	2262
ipv6 dhcp pool	2264
ipv6 dhcp server	2266
ipv6 local pool	2267
ipv6 nd prefix (DHCPv6)	2269
link-address	2271
option (DHCPv6)	2273
prefix-delegation pool	2275
service dhcp-relay	2277
show counter dhcp-relay	2278
show counter ipv6 dhcp-client	2281
show counter ipv6 dhcp-server	2283
show ip dhcp-relay	2285

	show ipv6 dhcp	2286
	show ipv6 dhcp binding	2287
	show ipv6 dhcp interface	2290
	show ipv6 dhcp pool	2292
	sntp-address	2294
Chapter 47:	Download Portal Commands	2295
	Introduction	2295
	aaa authentication download-portal	2296
	download-portal	2298
	download-portal reload	2299
	enable (download-portal)	2300
	file (download-portal)	2301
	http listen	2303
	http secure-listen	2305
	secure-listen (download-portal)	2307
	show download-portal	2309
	uri (download-portal)	2310
Chapter 48:	SNMP Commands	2311
	Introduction	2311
	alias (interface)	2313
	debug snmp	2314
	show counter snmp-server	2315
	show debugging snmp	2319
	show running-config snmp	2320
	show snmp-server	2321
	show snmp-server community	2322
	show snmp-server group	2323
	show snmp-server trap	2324
	show snmp-server user	2325
	show snmp-server view	2326
	snmp trap link-status	2327
	snmp trap link-status suppress	2328
	snmp-server	2330
	snmp-server community	2332
	snmp-server contact	2333
	snmp-server enable trap	2334
	snmp-server engineID local	2337
	snmp-server engineID local reset	2339
	snmp-server group	2340
	snmp-server host	2342
	snmp-server legacy-ifadminstatus	2344
	snmp-server location	2345
	snmp-server source-interface	2346
	snmp-server startup-trap-delay	2347
	snmp-server user	2348
	snmp-server view	2351
	test snmp trap snmp	2352
	undebg snmp	2353
Chapter 49:	Mail (SMTP) Commands	2354

	Introduction	2354
	debug mail	2355
	delete mail	2356
	mail	2357
	mail from	2359
	mail smtpserver	2360
	mail smtpserver authentication	2361
	mail smtpserver port	2363
	mail smtpserver tls	2365
	show counter mail	2366
	show mail	2367
	undebg mail	2368
Chapter 50:	RMON Commands	2369
	Introduction	2369
	rmon alarm	2370
	rmon collection history	2373
	rmon collection stats	2374
	rmon event	2375
	show rmon alarm	2376
	show rmon event	2377
	show rmon history	2379
	show rmon statistics	2381
Chapter 51:	Secure Shell (SSH) Commands	2383
	Introduction	2383
	banner login (SSH)	2385
	clear ssh	2386
	crypto key destroy hostkey	2387
	crypto key destroy userkey	2388
	crypto key generate hostkey	2389
	crypto key generate userkey	2391
	crypto key pubkey-chain knownhosts	2393
	crypto key pubkey-chain userkey	2395
	debug ssh client	2397
	debug ssh server	2398
	service ssh	2399
	show banner login	2401
	show crypto key hostkey	2402
	show crypto key pubkey-chain knownhosts	2404
	show crypto key pubkey-chain userkey	2406
	show crypto key userkey	2407
	show running-config ssh	2408
	show ssh	2410
	show ssh client	2412
	show ssh server	2413
	show ssh server allow-users	2415
	show ssh server deny-users	2416
	ssh	2417
	ssh client	2419
	ssh client allow-legacy-ssh-rsa	2421
	ssh server	2422

ssh server allow-legacy-ssh-rsa	2424
ssh server allow-users	2425
ssh server authentication	2427
ssh server deny-users	2429
ssh server max-auth-tries	2431
ssh server resolve-host	2432
ssh server scp	2433
ssh server secure-algs	2434
ssh server secure-ciphers	2435
ssh server secure-hostkey	2436
ssh server secure-kex	2437
ssh server secure-mac	2438
ssh server sftp	2439
ssh server tcpforwarding	2440
undebg ssh client	2441
undebg ssh server	2442

Chapter 52: Trigger Commands 2443

Introduction	2443
active (trigger)	2445
day	2446
debug trigger	2448
description (trigger)	2449
repeat	2450
script	2451
show debugging trigger	2453
show running-config trigger	2454
show trigger	2455
test	2460
time (trigger)	2461
trap	2463
trigger	2464
trigger activate	2465
type atmf guest	2466
type atmf node	2467
type cpu	2469
type interface	2470
type linkmon-probe	2471
type log	2473
type memory	2474
type periodic	2475
type ping-poll	2476
type reboot	2477
type time	2478
undebg trigger	2479

Chapter 53: Ping-Polling Commands 2480

Introduction	2480
active (ping-polling)	2482
clear ping-poll	2483
critical-interval	2484
debug ping-poll	2485

	description (ping-polling)	2486
	fail-count	2487
	ip (ping-polling)	2488
	length (ping-poll data)	2489
	normal-interval	2490
	ping-poll	2491
	sample-size	2492
	show counter ping-poll	2494
	show ping-poll	2496
	source-ip	2500
	timeout (ping polling)	2502
	up-count	2503
	undebg ping-poll	2504
Chapter 54:	sFlow Commands	2505
	Introduction	2505
	debug sflow	2506
	debug sflow agent	2507
	sflow agent	2508
	sflow collector	2510
	sflow collector id	2511
	sflow collector max-datagram-size	2513
	sflow enable	2514
	sflow max-header-size	2515
	sflow polling-interval	2517
	sflow sampling-rate	2518
	show debugging sflow	2519
	show running-config sflow	2520
	show sflow	2521
	show sflow interface	2523
	undebg sflow	2524
PART 8:	Firewall and Network Address Translation (NAT)	2525
Chapter 55:	Firewall Commands	2526
	Introduction	2526
	clear firewall connections	2528
	connection-limit (firewall)	2529
	connection-log events	2531
	debug firewall	2532
	firewall	2533
	geoip update-interval	2534
	ip subnet dynamic geoip	2535
	ipv6 subnet dynamic geoip	2536
	ip tcp timeout established	2537
	move rule (firewall)	2538
	protect (firewall)	2539
	rule (firewall)	2540
	show connection-log events	2543
	show firewall	2544
	show firewall connections	2545
	show firewall connections limits	2546

	show firewall connections limits config-check	2547
	show firewall rule	2548
	show firewall rule config-check	2550
	show debugging firewall	2551
	show running-config firewall	2552
Chapter 56:	Application and Entity Commands	2553
	Introduction	2553
	application	2555
	dport	2557
	dscp	2559
	host (network)	2561
	icmp-code	2563
	icmp-type	2565
	ip address (host)	2567
	ip subnet	2569
	ipv6 address (host)	2571
	ipv6 subnet	2573
	mac-address (host)	2575
	network (zone)	2577
	protocol	2579
	show application	2580
	show application detail	2581
	show entity	2584
	sport	2587
	zone	2589
Chapter 57:	NAT Commands	2591
	Introduction	2591
	enable (nat)	2593
	ip limited-local-proxy-arp	2594
	local-proxy-arp	2595
	move rule (nat)	2596
	nat	2597
	rule (nat)	2598
	show nat	2602
	show nat rule	2603
	show nat rule config-check	2605
	show running-config nat	2606
PART 9:	Advanced Network Protection	2607
Chapter 58:	IPS Commands	2608
	Introduction	2608
	alert-thresholding	2610
	category action (IPS)	2611
	ips	2612
	protect (IPS)	2613
	provider (IPS)	2614
	show ips	2615
	show ips categories	2616
	show ips categories detail	2618

	show running-config ips	2620
	sid	2621
	update-interval (IPS)	2622
Chapter 59:	Malware Protection Commands	2624
	Introduction	2624
	malware-protection	2625
	protect (malware)	2626
	provider kaspersky (malware)	2627
	show malware-protection	2628
	show running-config malware-protection	2629
	update-interval (malware)	2630
Chapter 60:	Antivirus Commands	2632
	Introduction	2632
	action (antivirus)	2634
	antivirus	2636
	dpi categorize	2637
	debug antivirus	2638
	protect (antivirus)	2639
	provider kaspersky (antivirus)	2640
	show antivirus	2641
	show antivirus statistics	2642
	show debugging antivirus	2643
	show running-config antivirus	2644
	update-interval (antivirus)	2645
Chapter 61:	URL Filtering Commands	2647
	Introduction	2647
	blacklist	2649
	log url-requests	2650
	protect (url-filter)	2651
	provider kaspersky (url-filter)	2652
	show running-config url-filter	2653
	show url-filter	2654
	update-interval (url-filter)	2655
	url-filter reload custom-lists	2657
	url-filter	2658
	whitelist (url-filter)	2659
Chapter 62:	Web Control Commands	2660
	Introduction	2660
	action (web-control)	2662
	bypass-web-control entity	2663
	category (web-control)	2665
	debug web-control	2667
	match (web-control)	2668
	move rule (web-control)	2670
	protect (web-control)	2671
	provider (web-control)	2672
	rule (web-control)	2673
	show debugging web-control	2675

	show running-config web-control	2676
	show web-control	2677
	show web-control bypass	2679
	show web-control categories	2680
	show web-control rules	2682
	web-control	2683
	web-control categorize	2685
Chapter 63:	Application Awareness Commands	2686
	Introduction	2686
	counters detailed	2687
	dpi	2688
	enable (dpi)	2689
	hostname (application)	2691
	provider (dpi)	2692
	show dpi	2693
	show dpi statistics	2695
	show running-config dpi	2697
	update-interval (dpi)	2698
	web-categorization	2699
Chapter 64:	IP Reputation Commands	2701
	Introduction	2701
	category action (IP Reputation)	2703
	ip-reputation	2705
	protect (IP Reputation)	2706
	provider proofpoint (IP Reputation)	2707
	show ip-reputation	2708
	show ip-reputation categories	2709
	show running-config ip-reputation	2711
	update-interval (IP Reputation)	2712
	whitelist (IP Reputation)	2714
PART 10:	Virtual Private Networks (VPNs)	2715
Chapter 65:	IPsec Commands	2716
	Introduction	2716
	clear isakmp sa	2718
	crypto ipsec profile	2719
	crypto isakmp key	2721
	crypto isakmp peer	2724
	crypto isakmp profile	2726
	debug isakmp	2728
	dpd-interval	2730
	dpd-timeout	2731
	interface tunnel (IPsec)	2732
	lifetime (IPsec Profile)	2733
	lifetime (ISAKMP Profile)	2734
	no debug isakmp	2735
	pfs	2736
	rekey	2738
	show debugging isakmp	2739

show interface tunnel (IPsec)	2740
show ipsec counters	2742
show ipsec peer	2743
show ipsec policy	2744
show ipsec profile	2745
show ipsec sa	2747
show isakmp counters	2748
show isakmp key (IPsec)	2749
show isakmp peer	2750
show isakmp profile	2751
show isakmp sa	2753
show tunnel inline-processing counters	2754
transform (IPsec Profile)	2756
transform (ISAKMP Profile)	2758
tunnel destination (IPsec)	2760
tunnel inline-processing	2762
tunnel local name (IPsec)	2763
tunnel local selector	2764
tunnel mode ipsec	2766
tunnel oper-status-control	2767
tunnel protection ipsec (IPsec)	2770
tunnel remote name (IPsec)	2771
tunnel remote selector	2772
tunnel security-reprocessing	2774
tunnel selector paired	2775
tunnel source (IPsec)	2776
undebg isakmp	2778
version (ISAKMP)	2779

Chapter 66: GRE Tunneling Commands 2780

Introduction	2780
interface tunnel (GRE)	2781
local authentication	2782
remote authentication	2784
show interface tunnel (GRE)	2786
tunnel checksum	2787
tunnel dscp	2788
tunnel destination (GRE)	2789
tunnel endpoint	2791
tunnel local name (GRE)	2793
tunnel mode gre	2794
tunnel mode gre multipoint	2795
tunnel protection ipsec (GRE)	2796
tunnel remote name (GRE)	2797
tunnel security-reprocessing	2798
tunnel source (GRE)	2799
tunnel ttl	2801

Chapter 67: OpenVPN Commands 2802

Introduction	2802
ip tcp adjust-mss	2804
ipv6 tcp adjust-mss	2806

show interface tunnel (OpenVPN)	2808
show openvpn connections	2809
show openvpn connections detail	2810
tunnel mode openvpn tap	2811
tunnel mode openvpn tun	2812
tunnel openvpn authentication	2813
tunnel openvpn cipher	2814
tunnel openvpn expiry-bytes	2816
tunnel openvpn expiry-seconds	2817
tunnel openvpn port	2818
tunnel openvpn route	2819
tunnel openvpn tagging	2821
tunnel openvpn tls-crypt	2822
tunnel openvpn tls-version-min	2823
tunnel openvpn verify-client-certificate trustpoint	2824
tunnel openvpn verify-client-certificate strict-common-name-check	2825
tunnel security-reprocessing	2827

Chapter 68: L2TPv3 Ethernet Pseudowire Commands 2828

Introduction	2828
interface tunnel (L2TPv3)	2829
l2tp unmanaged port	2830
show interface tunnel (L2TPv3)	2831
tunnel destination (L2TPv3)	2832
tunnel df	2834
tunnel local id	2835
tunnel mode l2tp v3	2836
tunnel protection ipsec	2837
tunnel remote id	2838
tunnel security-reprocessing	2839
tunnel source (L2TPv3)	2840

Chapter 69: Transitioning IPv4 to IPv6 Commands 2842

Introduction	2842
4to6-mapping	2844
br-address (software)	2845
clear 4to6-mapping	2846
ip dns forwarding dns46	2848
ip dns forwarding dns64	2850
limits (4to6-mapping)	2851
map4to6 (4to6-mapping)	2852
map6to4 (4to6-mapping)	2854
mesh-mode	2856
method	2857
originator (4to6-mapping) (deprecated)	2858
responder (4to6-mapping) (deprecated)	2859
rule	2860
show 4to6-mapping	2862
show ip dns forwarding dns46	2863
show running-config software-configuration	2864
show software-configuration	2865
software-configuration	2867

tunnel destination (DS-Lite)	2868
tunnel mode ds-lite	2869
tunnel mode lw4o6	2870
tunnel mode map-e	2871
tunnel security-reprocessing	2872
tunnel software	2873
upstream-interface	2874

Chapter 70:	IPv6 Tunneling Commands	2875
	Introduction	2875
	interface tunnel (IPv6)	2876
	ip address (IP Addressing and Protocol)	2877
	ip tcp adjust-mss	2879
	ipv6 address	2881
	ipv6 tcp adjust-mss	2883
	mtu	2885
	show interface tunnel (IPv6)	2887
	tunnel destination (IPv6)	2888
	tunnel dscp	2890
	tunnel mode (IPv6)	2891
	tunnel source (IPv6)	2892
	tunnel ttl	2894

List of Commands

2fa allow-reuse	1734
2fa create user email	1737
2fa create user skip-2fa	1738
2fa create user	1735
2fa delete user	1739
2fa email-expiry-time	1740
2fa email-otp	1741
2fa email-template	1742
2fa export user-data	1744
2fa hotp-window-size	1745
2fa import user-data source	1746
2fa issuer	1748
2fa label	1750
2fa max-skew	1752
2fa radius-email-attribute	1753
2fa reject-unconfigured-users	1755
2fa reset scratch-codes	1756
2fa reset skew	1757
2fa self-registration port	1761
2fa skew adjust	1758
2fa totp-window-size	1760
4to6-mapping	2844
aaa accounting commands	1580
aaa accounting login	1582
aaa accounting openvpn	1585

aaa accounting update	1587
aaa authentication 2fa-registration default group.....	1589
aaa authentication 2fa-registration default group.....	1763
aaa authentication download-portal	1591
aaa authentication download-portal	2296
aaa authentication enable default group tacacs+	1593
aaa authentication enable default local.....	1595
aaa authentication enable default local.....	169
aaa authentication isakmp	1596
aaa authentication login	1597
aaa authentication openvpn	1600
aaa authorization commands	1602
aaa authorization commands	1805
aaa authorization config-commands	1604
aaa authorization config-commands	1807
aaa group server.....	1605
aaa local authentication attempts logout-time.....	1607
aaa local authentication attempts logout-time.....	170
aaa local authentication attempts max-fail remote-login-only.....	1609
aaa local authentication attempts max-fail	1608
aaa local authentication attempts max-fail	171
aaa login fail-delay.....	1610
aaa login fail-delay.....	172
abr-type.....	833
accept-invalid-sslcert	512
accept-lifetime	643
accounting login	1611
action (antivirus).....	2634
action (web-control)	2662
activate	374
active (ping-polling)	2482
active (trigger).....	2445
address prefix	2232
address range	2234
address-family.....	924

advertisement-interval.....	1820
ageing-time	397
aggregate-address (IPv6 RIPng)	698
aggregate-address.....	926
alert-thresholding	2610
alias (interface)	2313
alliedware-behavior	645
alternate-checksum-mode	1822
antivirus.....	2636
application	2555
application-decision	1256
application-decision	1278
application-proxy ip-filter.....	1865
application-proxy quarantine-vlan	1866
application-proxy redirect-url	1867
application-proxy threat-protection send-summary.....	1870
application-proxy threat-protection.....	1868
application-proxy whitelist advertised-address	1871
application-proxy whitelist enable	1872
application-proxy whitelist protection tls.....	1873
application-proxy whitelist server	1874
application-proxy whitelist trustpoint (deprecated).....	1876
area authentication ipsec spi.....	834
area authentication.....	728
area default-cost (IPv6 OSPF).....	836
area default-cost.....	727
area encryption ipsec spi esp.....	837
area filter-list	729
area nssa	730
area range (IPv6 OSPF).....	840
area range.....	732
area stub (IPv6 OSPF)	842
area stub	734
area virtual-link (IPv6 OSPF)	843
area virtual-link authentication ipsec spi.....	845

area virtual-link encryption ipsec spi	847
area virtual-link	735
area-link	1877
arp log	463
arp opportunistic-nd	466
arp	462
arp-loose-check	467
arp-reply-bc-dmac	469
atmf amfplus-license-only	1882
atmf area password	1886
atmf area	1884
atmf authorize provision	1890
atmf authorize	1888
atmf backup area-masters delete	1893
atmf backup area-masters enable	1894
atmf backup area-masters now	1895
atmf backup area-masters synchronize	1896
atmf backup bandwidth	1897
atmf backup delete	1898
atmf backup enable	1899
atmf backup guests delete	1900
atmf backup guests enable	1901
atmf backup guests now	1902
atmf backup guests synchronize	1903
atmf backup now	1904
atmf backup redundancy enable	1906
atmf backup server	1907
atmf backup stop	1909
atmf backup synchronize	1910
atmf backup	1892
atmf cleanup	1911
atmf container login	1913
atmf container	1912
atmf controller	1914
atmf distribute firmware	1915

atmf domain vlan.....	1917
atmf enable	1920
atmf group (membership)	1921
atmf guest-class	1923
atmf log-verbose	1925
atmf management subnet	1926
atmf management vlan	1929
atmf master	1931
atmf mtu	1932
atmf network-name	1933
atmf provision (interface)	1934
atmf provision node	1935
atmf reboot-rolling	1937
atmf recover guest.....	1943
atmf recover led-off.....	1944
atmf recover over-eth.....	1945
atmf recover.....	1941
atmf recovery-server.....	1946
atmf remote-login	1948
atmf restricted-login.....	1950
atmf retry guest-link	1952
atmf secure-mode certificate expire	1955
atmf secure-mode certificate expiry	1956
atmf secure-mode certificate renew	1957
atmf secure-mode enable-all.....	1958
atmf secure-mode	1953
atmf select-area	1960
atmf topology-gui enable.....	111
atmf topology-gui enable.....	1961
atmf trustpoint	1962
atmf virtual-crosslink	1964
atmf virtual-link description.....	1969
atmf virtual-link protection	1970
atmf virtual-link	1966
atmf working-set	1972

atmf-arealink	1879
atmf-link	1881
attribute (radsrv-grp)	1687
authentication (ldap-server).....	1634
authentication.....	1689
auth-mac-promiscuous	1663
authorization commands	1612
authorization commands	1808
auto-cost reference bandwidth (IPv6 OSPF).....	850
auto-cost reference bandwidth	738
auto-summary (BGP only).....	929
bandwidth	740
bandwidth	852
banner display external-manager	240
banner exec	241
banner external-manager.....	243
banner login (SSH).....	2385
banner login (system).....	245
banner motd	247
base-dn	1636
bgp aggregate-nexthop-check.....	931
bgp always-compare-med	932
bgp bestpath as-path ignore.....	934
bgp bestpath compare-confed-aspath	935
bgp bestpath compare-routerid.....	936
bgp bestpath med remove-recv-med	939
bgp bestpath med remove-send-med.....	940
bgp bestpath med.....	937
bgp client-to-client reflection	941
bgp cluster-id	942
bgp confederation identifier	944
bgp confederation peers.....	945
bgp config-type	947
bgp dampening	949
bgp damp-peer-oscillation (BGP only).....	951

bgp default ipv4-unicast	952
bgp default local-preference (BGP only)	953
bgp deterministic-med	954
bgp enforce-first-as	956
bgp fast-external-failover	957
bgp graceful-restart graceful-reset	960
bgp graceful-restart	958
bgp log-neighbor-changes	961
bgp memory maxallocation	963
bgp nexthop-trigger delay	965
bgp nexthop-trigger enable	966
bgp nexthop-trigger-count	964
bgp rfc1771-path-select (BGP only)	967
bgp rfc1771-strict (BGP only)	968
bgp router-id	969
bgp scan-time (BGP only)	971
bgp update-delay	972
bind authenticate root-dn	1637
blacklist	2649
boot config-file backup	124
boot config-file	123
boot system backup	126
boot system	125
bootfile	2165
br-address (software)	2845
bridge	398
bridge-group (amf-container)	1974
bridge-group	399
browser-only (web-redirect)	217
bypass-web-control entity	2663
capability opaque	741
capability restart	742
category (web-control)	2665
category action (IP Reputation)	2703
category action (IPS)	2611

cd	127
circuit-failover	1823
cisco-metric-behavior (RIP)	647
class (htb)	1532
class (priority)	1534
class (wrr)	1536
clear 4to6-mapping	2846
clear aaa local user lockout	1614
clear aaa local user lockout	173
clear application-proxy threat-protection	1976
clear arp-cache	470
clear atmf links statistics	1979
clear atmf links virtual	1978
clear atmf links	1977
clear atmf recovery-file	1980
clear atmf secure-mode certificates	1981
clear atmf secure-mode statistics	1982
clear bgp (ASN)	976
clear bgp (IPv4 or IPv6 address)	974
clear bgp *	973
clear bgp external	977
clear bgp ipv6 (ASN) (BGP4+ only)	982
clear bgp ipv6 (ipv6 address) (BGP4+ only)	979
clear bgp ipv6 dampening (BGP4+ only)	980
clear bgp ipv6 external (BGP4+ only)	983
clear bgp ipv6 flap-statistics (BGP4+ only)	981
clear bgp ipv6 peer-group (BGP4+ only)	984
clear bgp peer-group	978
clear counter ipv6 dhcp-client	2236
clear counter ipv6 dhcp-server	2237
clear exception log	293
clear firewall connections	2528
clear ip bgp (ASN) (BGP only)	989
clear ip bgp (IPv4) (BGP only)	986
clear ip bgp * (BGP only)	985

clear ip bgp dampening (BGP only).....	987
clear ip bgp external (BGP only)	990
clear ip bgp flap-statistics (BGP only)	988
clear ip bgp peer-group (BGP only).....	991
clear ip dhcp binding	2166
clear ip dns forwarding cache	513
clear ip igmp group.....	1333
clear ip igmp interface	1334
clear ip igmp	1332
clear ip mroute pim sparse-mode	1418
clear ip mroute statistics	1383
clear ip mroute	1381
clear ip multicast route	1384
clear ip ospf process	743
clear ip pim sparse-mode bsr rp-set *	1416
clear ip pim sparse-mode packet statistics	1417
clear ip prefix-list	992
clear ip rip route	648
clear ipv6 dhcp binding.....	2238
clear ipv6 dhcp client	2240
clear ipv6 mld group.....	1363
clear ipv6 mld interface	1364
clear ipv6 mld	1362
clear ipv6 mroute pim sparse-mode.....	1470
clear ipv6 mroute pim	1469
clear ipv6 mroute statistics.....	1386
clear ipv6 mroute.....	1385
clear ipv6 neighbors	571
clear ipv6 ospf process.....	853
clear ipv6 pim sparse-mode bsr rp-set *	1471
clear ipv6 rip route.....	699
clear isakmp sa	2718
clear line vty.....	174
clear log buffered.....	295
clear log permanent	296

clear log.....	294
clear ping-poll.....	2483
clear radius local-server statistics.....	1695
clear snmp-discovery.....	2149
clear ssh.....	2386
clear stoat collector session counters.....	2129
client (pppoe-relay).....	453
client (radsecproxy-srv).....	1690
client mutual-authentication.....	1692
client name-check.....	1693
client trustpoint.....	1694
clock summer-time date.....	249
clock summer-time recurring.....	251
clock timezone.....	253
clone (amf-provision).....	1983
compatible rfc1583.....	744
configure boot config (amf-provision).....	1985
configure boot system (amf-provision).....	1987
configure terminal.....	100
connection-limit (firewall).....	2529
connection-log events.....	2531
connection-log events.....	297
consecutive probe loss.....	1280
copy (amf-provision).....	1989
copy (filename).....	128
copy buffered-log.....	298
copy debug.....	130
copy fdb-radius-users (to file).....	1696
copy local-radius-user-db (from file).....	1698
copy local-radius-user-db (to file).....	1699
copy permanent-log.....	299
copy running-config.....	131
copy startup-config.....	132
copy zmodem.....	133
counters detailed.....	2687

create (amf-provision)	1990
critical-interval	2484
crypto ipsec profile	2719
crypto isakmp key	2721
crypto isakmp peer	2724
crypto isakmp profile	2726
crypto key destroy hostkey.	2387
crypto key destroy userkey.	2388
crypto key generate hostkey	2389
crypto key generate rsa	1778
crypto key generate userkey	2391
crypto key pubkey-chain knownhosts	2393
crypto key pubkey-chain userkey.	2395
crypto key zeroize	1779
crypto pki authenticate	1780
crypto pki enroll local (deleted)	1700
crypto pki enroll local local-radius-all-users (deleted)	1701
crypto pki enroll local user (deleted).	1702
crypto pki enroll user	1782
crypto pki enroll	1781
crypto pki export local pem (deleted)	1703
crypto pki export local pkcs12 (deleted)	1704
crypto pki export pem	1784
crypto pki export pkcs12	1785
crypto pki import pem	1787
crypto pki import pkcs12	1789
crypto pki trustpoint local (deleted)	1705
crypto pki trustpoint	1790
custom-failure	514
custom-success	515
day	2446
ddns enable	516
ddns-update now	519
ddns-update-method	517
deadtime (ldap-server)	1638

deadtime (RADIUS server group)	1664
debug 2fa	1765
debug aaa	1615
debug antivirus	2638
debug atmf packet	1994
debug atmf	1992
debug bgp (BGP only)	993
debug core-file	254
debug crypto pki (deleted)	1706
debug ddns	520
debug firewall	2532
debug igmp	1335
debug ip dns forwarding	521
debug ip packet interface	471
debug ipv6 ospf events	854
debug ipv6 ospf ifsm	855
debug ipv6 ospf lsa	856
debug ipv6 ospf nfm	857
debug ipv6 ospf packet	858
debug ipv6 ospf route	859
debug ipv6 pim sparse-mode packet	1474
debug ipv6 pim sparse-mode timer	1475
debug ipv6 pim sparse-mode	1472
debug ipv6 rip	700
debug isakmp	2728
debug ldap client	1639
debug linkmon	1282
debug mail	2355
debug mld	1365
debug nsm mcast	1388
debug nsm mcast6	1389
debug nsm	1387
debug ospf events	745
debug ospf ifsm	746
debug ospf lsa	747

debug ospf nfsm	748
debug ospf nsm	749
debug ospf packet.....	750
debug ospf route	751
debug pim sparse-mode timer	1420
debug pim sparse-mode.....	1419
debug ping-poll	2485
debug policy-based-routing	1258
debug ppp	411
debug radius	1665
debug rip	649
debug sflow agent.....	2507
debug sflow	2506
debug snmp.....	2314
debug ssh client	2397
debug ssh server	2398
debug traffic-control.....	1538
debug trigger	2448
debug vrrp events	1826
debug vrrp packet.....	1827
debug vrrp	1825
debug web-control	2667
default log buffered	300
default log console	301
default log email	302
default log host.....	303
default log monitor.....	304
default log permanent.....	305
default-information originate (IPv6 RIPng).....	701
default-information originate (RIP)	650
default-information originate	752
default-information originate	860
default-metric (IPv6 OSPF)	861
default-metric (IPv6 RIPng).....	702
default-metric (OSPF)	753

default-metric (RIP)	651
default-router	2167
delete (amf-provision)	1997
delete debug	135
delete mail	2356
delete	134
description (amf-container)	2001
description (domain-list)	522
description (interface)	378
description (ping-polling)	2486
description (stoat-dest)	2130
description (trigger)	2449
destination (linkmon-probe)	1284
dir	136
disable (Privileged Exec mode)	101
disable (VRRP)	1828
discovery	1999
distance (BGP and BGP4+)	995
distance (IPv6 OSPF)	862
distance (OSPF)	754
distance (RIP)	652
distribute-list (IPv6 RIPng)	703
distribute-list (OSPF)	756
distribute-list (RIP)	653
dns-server (DHCPv6)	2241
dns-server	2168
do	102
domain	523
domain-name (DHCPv6)	2243
domain-name	2169
domain-style	1707
download-portal reload	2299
download-portal	2298
dpd-interval	2730
dpd-timeout	2731

dpi categorize	2637
dpi	2688
dport	2557
dscp (linkmon-probe)	1286
dscp	2559
echo	375
edit	138
egress interface (linkmon-probe)	1287
egress-vlan-id (radsrv-grp)	1708
egress-vlan-name (radsrv-grp)	1709
email-attribute (ldap-server)	1766
enable (download-portal)	2300
enable (dpi)	2689
enable (linkmon-probe)	1288
enable (nat)	2593
enable (Privileged Exec mode)	103
enable (VRRP)	1829
enable (web-redirect)	218
enable db-summary-opt	758
enable password	175
enable secret (deprecated)	177
encapsulation dot1q	407
encapsulation ppp	414
end	105
enrollment (ca-trustpoint)	1791
erase factory-default	139
erase factory-default	2002
erase startup-config	140
exclude app	219
exclude dst-ip	221
exclude ip	223
exclude mac	224
exclude url	225
exec-timeout	178
exit	106

exit-address-family	997
expect-html-response	524
fail-count.....	2487
file (download-portal).....	2301
fingerprint (ca-trustpoint).....	1792
firewall	2533
firmware-url	2003
follow-redirects.....	525
fullupdate (RIP)	654
geoip update-interval.....	2534
get-before-submit	526
get-params	527
group (radsrv)	1710
group-attribute.....	1641
group-dn.....	1642
help radius-attribute.....	1711
help.....	107
host (DHCP)	2170
host (ldap-server).....	1643
host (network).....	2561
host area	759
hostname (application)	2691
host-name (ddns-update-method)	528
hostname	255
http listen	2303
http log webapi-requests	112
http port	113
http secure-listen	2305
http secure-port	114
http trustpoint	115
http-enable	2005
icmp-code.....	2563
icmp-type	2565
identity (amf-provision).....	2007
idle-time (web-redirect).....	227

interface (PPP).....	415
interface (to configure)	379
interface (traffic-control)	1539
interface dynamic-virtual-bandwidth.....	1541
interface tunnel (GRE).....	2781
interface tunnel (IPsec).....	2732
interface tunnel (IPv6)	2876
interface tunnel (L2TPv3)	2829
interval (linkmon-probe)	1289
ip (ping-polling)	2488
ip address (host).....	2567
ip address (IP Addressing and Protocol)	2877
ip address (IP Addressing and Protocol)	473
ip address dhcp	2171
ip address negotiated.....	416
ip community-list expanded	1000
ip community-list standard	1002
ip community-list.....	998
ip ddns-update-method	529
ip dhcp bootp ignore	2173
ip dhcp leasequery enable	2174
ip dhcp option.....	2175
ip dhcp pool.....	2177
ip dhcp-client default-route distance	2178
ip dhcp-client request vendor-identifying-specific	2180
ip dhcp-client vendor-identifying-class	2181
ip dhcp-relay agent-option checking	2184
ip dhcp-relay agent-option checking	2246
ip dhcp-relay agent-option remote-id	2185
ip dhcp-relay agent-option remote-id	2247
ip dhcp-relay agent-option	2182
ip dhcp-relay agent-option	2244
ip dhcp-relay information policy	2186
ip dhcp-relay information policy	2248
ip dhcp-relay maxhops	2188

ip dhcp-relay maxhops	2250
ip dhcp-relay max-message-length.....	2189
ip dhcp-relay max-message-length.....	2251
ip dhcp-relay server-address	2191
ip dhcp-relay server-address	2253
ip dhcp-relay short-lease.....	2193
ip dhcp-relay short-lease-ipv6.....	2255
ip dhcp-relay use-client-side-address.....	2194
ip directed-broadcast.....	475
ip dns forwarding cache	531
ip dns forwarding dead-time.....	532
ip dns forwarding dns46	2848
ip dns forwarding dns64	2850
ip dns forwarding domain-list.....	533
ip dns forwarding retry	534
ip dns forwarding source-interface	535
ip dns forwarding timeout	536
ip dns forwarding.....	530
ip domain-list.....	537
ip domain-lookup	538
ip domain-name.....	540
ip extcommunity-list expanded	1004
ip extcommunity-list standard	1006
ip forwarding.....	477
ip forward-protocol udp	478
ip helper-address.....	480
ip icmp error-interval	482
ip icmp-timestamp	483
ip igmp last-member-query-count	1337
ip igmp last-member-query-interval.....	1338
ip igmp mroute-proxy	1339
ip igmp proxy-service.....	1340
ip igmp querier-timeout	1341
ip igmp query-holdtime	1342
ip igmp query-interval	1344

ip igmp query-max-response-time	1346
ip igmp ra-option	1348
ip igmp robustness-variable	1349
ip igmp source-address-check	1350
ip igmp startup-query-count	1351
ip igmp startup-query-interval	1352
ip igmp version	1353
ip igmp	1336
ip limited-local-proxy-arp	2594
ip limited-local-proxy-arp	484
ip local-proxy-arp	485
ip mroute	1390
ip multicast handle-igmp-immediately	1392
ip multicast route	1393
ip multicast route-limit	1395
ip multicast wrong-vif-suppression	1396
ip multicast-routing	1397
ip name-server preferred-order	543
ip name-server	541
ip ospf authentication	760
ip ospf authentication-key	761
ip ospf cost	762
ip ospf database-filter	763
ip ospf dead-interval	764
ip ospf disable all	765
ip ospf hello-interval	766
ip ospf message-digest-key	767
ip ospf mtu	769
ip ospf mtu-ignore	770
ip ospf network	771
ip ospf priority	772
ip ospf resync-timeout	773
ip ospf retransmit-interval	774
ip ospf transmit-delay	775
ip pim anycast-rp	1422

ip pim bsr-border	1423
ip pim bsr-candidate	1424
ip pim cisco-register-checksum	1425
ip pim crp-cisco-prefix	1426
ip pim dr-priority	1427
ip pim exclude-genid	1428
ip pim ext-srcs-directly-connected	1429
ip pim hello-holdtime (PIM-SM)	1430
ip pim hello-interval (PIM-SM)	1431
ip pim ignore-rp-set-priority	1432
ip pim jp-timer	1433
ip pim register-rate-limit	1434
ip pim register-rp-reachability	1435
ip pim register-source	1436
ip pim register-suppression	1437
ip pim rp-address	1438
ip pim rp-candidate	1440
ip pim rp-register-kat	1441
ip pim sparse-mode join-prune-batching	1443
ip pim sparse-mode passive	1444
ip pim sparse-mode wrong-vif-suppression	1445
ip pim sparse-mode	1442
ip pim spt-threshold	1446
ip pim ssm	1447
ip policy-route	1259
ip policy-route	1290
ip prefix-list	1008
ip prefix-list	656
ip proxy-arp	486
ip radius require-message-authenticator	1666
ip radius source-interface	1667
ip redirects	487
ip resolve-via-default	622
ip rip authentication key-chain	658
ip rip authentication mode	660

ip rip authentication string	662
ip rip receive version	665
ip rip receive-packet	664
ip rip send version 1-compatible	669
ip rip send version	667
ip rip send-packet	666
ip rip split-horizon	670
ip route	623
ip subnet dynamic geoip	2535
ip subnet	2569
ip summary-address rip	655
ip tacacs source-interface	1810
ip tcp adjust-mss	2804
ip tcp adjust-mss	2879
ip tcp adjust-mss	381
ip tcp adjust-mss	418
ip tcp synack-retries	488
ip tcp timeout established	2537
ip tcp timeout established	489
ip tcp-timestamp	490
ip tftp source-interface	141
ip unnumbered	420
ip unreachable	491
ip-reputation	2705
ips	2612
ipv6 address (DHCPv6 PD)	2256
ipv6 address (host)	2571
ipv6 address autoconfig	574
ipv6 address dhcp	2258
ipv6 address suffix	576
ipv6 address	2881
ipv6 address	572
ipv6 ddns-update-method	544
ipv6 dhcp client pd	2260
ipv6 dhcp option	2262

ipv6 dhcp pool	2264
ipv6 dhcp server	2266
ipv6 enable	577
ipv6 eui64-linklocal	579
ipv6 forwarding	580
ipv6 icmp error-interval	581
ipv6 local pool	2267
ipv6 mld last-member-query-count	1367
ipv6 mld last-member-query-interval	1368
ipv6 mld querier-timeout	1369
ipv6 mld query-interval	1370
ipv6 mld query-max-response-time	1371
ipv6 mld robustness-variable	1372
ipv6 mld static-group	1373
ipv6 mld version	1374
ipv6 mld	1366
ipv6 mroute	1398
ipv6 multicast forward-slow-path-packet	582
ipv6 multicast route	1400
ipv6 multicast route-limit	1402
ipv6 multicast-routing	1403
ipv6 multihoming	583
ipv6 nd accept-ra-default-routes	584
ipv6 nd accept-ra-pinfo	585
ipv6 nd current-hoplimit	586
ipv6 nd dns search-list	588
ipv6 nd dns-server	589
ipv6 nd managed-config-flag	591
ipv6 nd minimum-ra-interval	592
ipv6 nd other-config-flag	594
ipv6 nd prefix (DHCPv6)	2269
ipv6 nd prefix	595
ipv6 nd proxy interface	597
ipv6 nd ra-interval	598
ipv6 nd ra-lifetime	599

ipv6 nd reachable-time	601
ipv6 nd retransmission-time	603
ipv6 nd route-information	605
ipv6 nd router-preference.....	606
ipv6 nd suppress-ra.....	607
ipv6 opportunistic-nd.....	608
ipv6 ospf authentication spi.....	864
ipv6 ospf cost	866
ipv6 ospf dead-interval	867
ipv6 ospf display route single-line	868
ipv6 ospf encryption spi esp	869
ipv6 ospf hello-interval	872
ipv6 ospf neighbor	873
ipv6 ospf network	875
ipv6 ospf priority	876
ipv6 ospf retransmit-interval	877
ipv6 ospf transmit-delay	878
ipv6 pim anycast-rp.....	1477
ipv6 pim bsr-border	1479
ipv6 pim bsr-candidate	1481
ipv6 pim cisco-register-checksum	1483
ipv6 pim crp-cisco-prefix.....	1484
ipv6 pim dr-priority.....	1485
ipv6 pim exclude-genid.....	1487
ipv6 pim ext-srccs-directly-connected.....	1488
ipv6 pim hello-holdtime	1489
ipv6 pim hello-interval.....	1491
ipv6 pim ignore-rp-set-priority	1492
ipv6 pim jp-timer	1493
ipv6 pim register-rate-limit.....	1494
ipv6 pim register-rp-reachability	1495
ipv6 pim register-source	1496
ipv6 pim register-suppression.....	1498
ipv6 pim rp embedded	1501
ipv6 pim rp-address	1499

ipv6 pim rp-candidate	1500
ipv6 pim rp-register-kat.....	1502
ipv6 pim sparse-mode passive	1504
ipv6 pim sparse-mode	1503
ipv6 pim spt-threshold.....	1505
ipv6 pim ssm	1506
ipv6 pim unicast-bsm.....	1507
ipv6 policy-route	1261
ipv6 policy-route	1293
ipv6 prefix-list	1010
ipv6 prefix-list	704
ipv6 rip metric-offset	706
ipv6 rip split-horizon.....	708
ipv6 route	609
ipv6 route	626
ipv6 router ospf area.....	879
ipv6 router rip	709
ipv6 subnet dynamic geoip	2536
ipv6 subnet	2573
ipv6 tcp adjust-mss	2806
ipv6 tcp adjust-mss	2883
ipv6 tcp adjust-mss	383
ipv6 tcp adjust-mss	422
ipv6 tftp source-interface	142
ipv6 unreachable	611
ip-version (linkmon-probe).....	1292
jitter.....	1295
keepalive (PPP)	424
key (stoat-dest)	2131
key chain.....	672
key.....	671
key-string	673
l2tp unmanaged port.....	2830
l3-filtering enable.....	1543
l3-filtering enable.....	401

latency	1297
ldap-server	1645
lease	2195
length (asyn)	179
length (ping-poll data)	2489
license update file	209
license update online	210
license-cert (amf-provision)	2009
lifetime (IPsec Profile)	2733
lifetime (ISAKMP Profile)	2734
limits (4to6-mapping)	2851
line	180
link-address	2271
linkmon group	1299
linkmon probe	1302
linkmon probe-history	1300
linkmon profile	1304
load-balancing	1305
local authentication	2782
local-proxy-arp	2595
local-proxy-arp	493
locate (amf-provision)	2011
log buffered (filter)	307
log buffered exclude	310
log buffered size	313
log buffered	306
log console (filter)	315
log console exclude	318
log console	314
log date-format	321
log email (filter)	323
log email exclude	326
log email time	329
log email	322
log event-host	117

log event-host.....	2013
log facility	331
log host (filter).....	335
log host exclude.....	338
log host source	341
log host startup-delay	342
log host time	344
log host	333
log monitor (filter)	346
log monitor exclude	349
log permanent (filter)	353
log permanent exclude	356
log permanent size	359
log permanent	352
log trustpoint.....	361
log url-requests.....	2650
log url-requests.....	362
login authentication	1616
login-attribute.....	1647
login-fallback enable	2014
logout.....	108
log-rate-limit nsm	360
low-memory restart.....	257
mac-address (host)	2575
mac-learning	402
mail from.....	2359
mail smtpserver authentication	2361
mail smtpserver port.....	2363
mail smtpserver tls.....	2365
mail smtpserver	2360
mail	2357
malware-protection	2625
map4to6 (4to6-mapping)	2852
map6to4 (4to6-mapping)	2854
match (web-control).....	2668

match as-path	1012
match as-path	1215
match community	1013
match community	1216
match interface	1218
match ip address	1219
match ip next-hop	1221
match ipv6 address	1223
match ipv6 next-hop	1225
match metric	1226
match origin	1227
match route-type	1229
match tag	1230
max-concurrent-dd (IPv6 OSPF)	881
max-concurrent-dd	776
max-fib-routes	258
max-fib-routes	628
maximum-area	777
maximum-paths	630
maximum-prefix	674
max-paths	1015
max-sessions	454
max-static-routes	259
max-static-routes	629
member (linkmon-group)	1306
mesh-mode	2856
method	2857
mkdir	143
mode (web-redirect)	229
modeltype	2015
move debug	145
move rule (firewall)	2538
move rule (nat)	2596
move rule (traffic-control)	1544
move rule (web-control)	2670

move.....	144
mtu (PPP)	426
mtu	2885
mtu	385
name-check (stoat-dest)	2132
nas message-authenticator (radsvr)	1714
nas.....	1713
nat	2597
neighbor (IPv6 RIPng).....	710
neighbor (OSPF)	778
neighbor (RIP)	675
neighbor activate.....	1016
neighbor advertisement-interval.....	1019
neighbor allowas-in	1022
neighbor as-origination-interval	1025
neighbor attribute-unchanged.....	1027
neighbor capability graceful-restart	1030
neighbor capability orf prefix-list.....	1033
neighbor capability route-refresh	1036
neighbor collide-established.....	1039
neighbor default-originate.....	1042
neighbor description	1045
neighbor disallow-infinite-holdtime.....	1048
neighbor dont-capability-negotiate	1050
neighbor ebgp-multihop	1053
neighbor enforce-multihop	1056
neighbor filter-list	1059
neighbor interface.....	1062
neighbor local-as	1064
neighbor maximum-prefix	1067
neighbor next-hop-self	1070
neighbor override-capability.....	1073
neighbor passive	1075
neighbor password.....	1078
neighbor peer-group (add a neighbor)	1081

neighbor peer-group (create a peer-group).....	1083
neighbor port	1084
neighbor prefix-list	1087
neighbor remote-as	1090
neighbor remove-private-AS (BGP only)	1093
neighbor restart-time.....	1095
neighbor route-map	1098
neighbor route-reflector-client (BGP only)	1102
neighbor route-server-client (BGP only)	1104
neighbor send-community.....	1105
neighbor shutdown	1109
neighbor soft-reconfiguration inbound.....	1111
neighbor timers	1114
neighbor transparent-as	1117
neighbor transparent-nexthop.....	1119
neighbor unsuppress-map.....	1121
neighbor update-source	1124
neighbor version (BGP only)	1128
neighbor weight.....	1130
network (BGP and BGP4+)	1133
network (DHCP)	2197
network (RIP)	676
network (zone)	2577
network area	779
network synchronization.....	1136
next-server	2198
no crypto pki certificate.....	1794
no debug all.....	260
no debug isakmp.....	2735
normal-interval.....	2490
obey-form.....	545
option (DHCPv6).....	2273
option.....	2199
originator (4to6-mapping) (deprecated).....	2858
ospf abr-type	781

ospf restart grace-period	782
ospf restart helper	783
ospf router-id	785
overflow database external	787
overflow database	786
passive-interface (IPv6 OSPF)	882
passive-interface (IPv6 RIPng)	711
passive-interface (OSPF)	788
passive-interface (RIP)	677
password (ddns-update-method)	546
peer default ip address	427
peer neighbor-route	429
pfs	2736
ping ipv6	612
ping	494
ping-poll	2491
pktloss	1308
policy (traffic-control)	1545
policy-based-routing enable	1264
policy-based-routing	1263
port (ldap-server)	1649
ppp authentication refuse	433
ppp authentication	431
ppp hostname	435
ppp ipcp dns suffix-list	439
ppp ipcp dns suffix-list	549
ppp ipcp dns	437
ppp ipcp dns	547
ppp ipcp ip-override	441
ppp password	442
ppp service-name (PPPoE)	443
ppp timeout idle	444
ppp username	445
pppoe-relay	455
preempt-mode	1830

preference	1310
prefix-delegation pool	2275
priority	1832
privilege level	181
probe enable	2201
probe packets	2202
probe timeout	2203
probe type	2204
protect (antivirus)	2639
protect (firewall)	2539
protect (IP Reputation)	2706
protect (IPS)	2613
protect (malware)	2626
protect (url-filter)	2651
protect (web-control)	2671
protocol	2579
provider (dpi)	2692
provider (IPS)	2614
provider (web-control)	2672
provider kaspersky (antivirus)	2640
provider kaspersky (malware)	2627
provider kaspersky (url-filter)	2652
provider proofpoint (IP Reputation)	2707
proxy-host (web-redirect)	231
proxy-port	1617
pwd	146
radius-secure-proxy aaa	1618
radius-secure-proxy local-server	1716
radius-server deadtime	1668
radius-server host	1669
radius-server key	1672
radius-server local	1717
radius-server retransmit	1673
radius-server timeout	1675
range	2205

reboot	262
recv-buffer-size (IPv6 RIPng)	712
recv-buffer-size (RIP)	678
red-curve	1547
redistribute (into BGP or BGP4+)	1137
redistribute (IPv6 OSPF)	883
redistribute (IPv6 RIPng)	713
redistribute (OSPF)	789
redistribute (RIP)	679
rekey	2738
reload	263
remote authentication	2784
repeat	2450
repeat-time (web-redirect)	233
responder (4to6-mapping) (deprecated)	2859
restart bgp graceful (BGP only)	1139
restart ipv6 ospf graceful	885
restart ospf graceful	791
restart rip graceful	680
retransmit (ldap-server)	1650
retry-interval	551
rip restart grace-period	681
rmdir	147
rmon alarm	2370
rmon collection history	2373
rmon collection stats	2374
rmon event	2375
route (IPv6 RIPng)	714
route (RIP)	682
route	2206
route-map	1141
route-map	1231
router bgp	1140
router ipv6 ospf	886
router ipv6 rip	715

router ipv6 vrrp (interface)	1834
router ospf	792
router rip	683
router vrrp (interface)	1836
router-id (IPv6 OSPF)	887
router-id	793
rsakeypair (ca-trustpoint)	1795
rule (firewall)	2540
rule (nat)	2598
rule (traffic-control)	1549
rule (web-control)	2673
rule	2860
sample-size (linkmon-probe)	1312
sample-size	2492
script	2451
search-filter	1651
secure cipher (ldap-server)	1653
secure mode (ldap-server)	1655
secure trustpoint (ldap-server)	1657
secure-listen (download-portal)	2307
security-password forced-change	183
security-password history	182
security-password lifetime	184
security-password minimum-categories	186
security-password minimum-length	187
security-password min-lifetime-enforce	185
security-password reject-expired-pwd	188
security-password warning	189
send-lifetime	684
server (ldap-group)	1658
server (pppoe-relay)	456
server (RADIUS server group)	1677
server (radsecproxy-aaa)	1619
server auth-port	1718
server enable	1719

server mutual-authentication	1621
server name-check	1622
server trustpoint (radsrv)	1720
server trustpoint	1623
server-url (web-redirect)	234
service 2fa	1767
service advanced-vty	190
service atmf-application-proxy	2016
service dhcp-relay	2207
service dhcp-relay	2277
service dhcp-server	2208
service http	118
service password-encryption	191
service pim	1448
service pim6	1508
service snmp-discovery	2150
service ssh	2399
service statistics interfaces counter	387
service stoat	2133
service telnet	192
set aggregator	1234
set as-path	1144
set as-path	1235
set atomic-aggregate	1236
set comm-list delete	1237
set community	1145
set community	1238
set dampening	1240
set extcommunity	1242
set ip next-hop (route map)	1244
set ipv6 next-hop	1245
set local-preference	1246
set metric	1247
set metric-type	1249
set origin	1250

set originator-id	1251
set tag	1252
set weight	1253
sflow agent	2508
sflow collector id	2511
sflow collector max-datagram-size	2513
sflow collector	2510
sflow enable	2514
sflow max-header-size	2515
sflow polling-interval	2517
sflow sampling-rate	2518
short-lease-threshold	2209
show 2fa email-template	1770
show 2fa user	1771
show 2fa users	1773
show 2fa	1769
show 4to6-mapping	2862
show aaa local user locked	1625
show aaa local user locked	193
show aaa server group	1627
show antivirus statistics	2642
show antivirus	2641
show application detail	2581
show application	2580
show application-proxy threat-protection	2017
show application-proxy whitelist advertised-address	2019
show application-proxy whitelist interface	2020
show application-proxy whitelist server	2022
show application-proxy whitelist supplicant	2023
show arp	495
show atmf area guests	2032
show atmf area guests-detail	2034
show atmf area nodes	2036
show atmf area nodes-detail	2038
show atmf area summary	2040

show atmf area	2029
show atmf authorization	2041
show atmf backup area	2048
show atmf backup guest	2050
show atmf backup	2044
show atmf container	2052
show atmf detail	2055
show atmf group members	2059
show atmf group	2057
show atmf guests detail	2063
show atmf guests	2061
show atmf links detail	2068
show atmf links guest detail	2079
show atmf links guest	2077
show atmf links statistics	2083
show atmf links	2066
show atmf nodes	2086
show atmf provision nodes	2088
show atmf recovery-file	2090
show atmf secure-mode audit link	2094
show atmf secure-mode audit	2093
show atmf secure-mode certificates	2095
show atmf secure-mode sa	2098
show atmf secure-mode statistics	2101
show atmf secure-mode	2091
show atmf tech	2103
show atmf virtual-links	2106
show atmf working-set	2108
show atmf	2025
show banner external-manager	264
show banner login	2401
show bgp ipv6 (BGP4+ only)	1147
show bgp ipv6 community (BGP4+ only)	1148
show bgp ipv6 community-list (BGP4+ only)	1150
show bgp ipv6 dampening (BGP4+ only)	1151

show bgp ipv6 filter-list (BGP4+ only)	1152
show bgp ipv6 inconsistent-as (BGP4+ only).....	1153
show bgp ipv6 longer-prefixes (BGP4+ only).....	1154
show bgp ipv6 neighbors (BGP4+ only)	1155
show bgp ipv6 paths (BGP4+ only)	1158
show bgp ipv6 prefix-list (BGP4+ only)	1159
show bgp ipv6 quote-regexp (BGP4+ only)	1160
show bgp ipv6 regexp (BGP4+ only).....	1161
show bgp ipv6 route-map (BGP4+ only)	1163
show bgp ipv6 summary (BGP4+ only)	1164
show bgp memory maxallocation (BGP only)	1165
show bgp nexthop-tracking (BGP only).....	1166
show bgp nexthop-tree-details (BGP only).....	1167
show boot.....	148
show bridge macaddr	405
show bridge.....	403
show clock	265
show connection-log events	2543
show connection-log events	363
show counter dhcp-client.....	2211
show counter dhcp-relay	2212
show counter dhcp-relay	2278
show counter dhcp-server	2215
show counter ipv6 dhcp-client.....	2281
show counter ipv6 dhcp-server	2283
show counter log	364
show counter mail.....	2366
show counter ping-poll	2494
show counter snmp-server.....	2315
show cpu history	270
show cpu.....	267
show crypto key hostkey.....	2402
show crypto key mypubkey rsa.....	1796
show crypto key pubkey-chain knownhosts	2404
show crypto key pubkey-chain userkey.....	2406

show crypto key userkey	2407
show crypto pki certificates	1797
show crypto pki enrollment user	1799
show crypto pki trustpoint	1800
show ddns-update-method status	552
show debugging 2fa	1774
show debugging aaa	1628
show debugging antivirus	2643
show debugging atmf packet	2110
show debugging atmf	2109
show debugging bgp (BGP only)	1168
show debugging firewall	2551
show debugging igmp	1354
show debugging ip dns forwarding	553
show debugging ip packet	497
show debugging ipv6 ospf	888
show debugging ipv6 pim sparse-mode	1509
show debugging ipv6 rip	716
show debugging isakmp	2739
show debugging linkmon	1313
show debugging mld	1375
show debugging nsm mcast	1404
show debugging ospf	794
show debugging pim sparse-mode	1449
show debugging ppp	446
show debugging radius	1679
show debugging rip	686
show debugging sflow	2519
show debugging snmp	2319
show debugging traffic-control	1551
show debugging trigger	2453
show debugging vrrp	1838
show debugging web-control	2675
show debugging	272
show dhcp lease	2217

show download-portal.....	2309
show dpi statistics	2695
show dpi	2693
show entity.....	2584
show exception log.....	365
show file systems	151
show file	150
show firewall connections limits config-check	2547
show firewall connections limits	2546
show firewall connections	2545
show firewall rule config-check	2550
show firewall rule.....	2548
show firewall	2544
show hash.....	149
show hash.....	1801
show history.....	109
show hosts	554
show http	119
show interface (PPP)	447
show interface brief.....	391
show interface status	392
show interface tunnel (GRE).....	2786
show interface tunnel (IPsec).....	2740
show interface tunnel (IPv6).....	2887
show interface tunnel (L2TPv3).....	2831
show interface tunnel (OpenVPN)	2808
show interface.....	388
show ip bgp (BGP only)	1169
show ip bgp attribute-info (BGP only)	1170
show ip bgp cidr-only (BGP only).....	1171
show ip bgp community (BGP only)	1172
show ip bgp community-info (BGP only).....	1174
show ip bgp community-list (BGP only).....	1175
show ip bgp dampening (BGP only)	1176
show ip bgp filter-list (BGP only)	1178

show ip bgp inconsistent-as (BGP only).....	1179
show ip bgp longer-prefixes (BGP only).....	1180
show ip bgp neighbors (BGP only)	1181
show ip bgp neighbors connection-retrytime (BGP only).....	1184
show ip bgp neighbors hold-time (BGP only)	1185
show ip bgp neighbors keepalive (BGP only)	1186
show ip bgp neighbors keepalive-interval (BGP only)	1187
show ip bgp neighbors notification (BGP only).....	1188
show ip bgp neighbors open (BGP only).....	1189
show ip bgp neighbors rcvd-msgs (BGP only).....	1190
show ip bgp neighbors sent-msgs (BGP only).....	1191
show ip bgp neighbors update (BGP only).....	1192
show ip bgp paths (BGP only)	1193
show ip bgp prefix-list (BGP only)	1194
show ip bgp quote-regexp (BGP only)	1195
show ip bgp regexp (BGP only).....	1197
show ip bgp route-map (BGP only)	1199
show ip bgp scan (BGP only)	1200
show ip bgp summary (BGP only)	1201
show ip community-list.....	1202
show ip dhcp binding.....	2218
show ip dhcp pool.....	2220
show ip dhcp server statistics	2226
show ip dhcp server summary	2228
show ip dhcp-relay	2225
show ip dhcp-relay	2285
show ip dns forwarding cache	556
show ip dns forwarding dns46	2863
show ip dns forwarding server	557
show ip dns forwarding.....	555
show ip domain-list.....	558
show ip domain-name.....	559
show ip extcommunity-list.....	1203
show ip flooding-nexthops	498
show ip forwarding	499

show ip igmp groups	1355
show ip igmp interface	1357
show ip interface	500
show ip mroute.....	1405
show ip mvif.....	1408
show ip name-server.....	560
show ip ospf border-routers.....	798
show ip ospf database asbr-summary	801
show ip ospf database external	802
show ip ospf database network	804
show ip ospf database nssa-external	805
show ip ospf database opaque-area.....	807
show ip ospf database opaque-as	808
show ip ospf database opaque-link.....	809
show ip ospf database router	810
show ip ospf database summary	812
show ip ospf database	799
show ip ospf interface	815
show ip ospf neighbor	816
show ip ospf route.....	818
show ip ospf virtual-links.....	819
show ip ospf.....	795
show ip pbr route.....	1265
show ip pim sparse-mode bsr-router	1450
show ip pim sparse-mode interface detail	1453
show ip pim sparse-mode interface	1451
show ip pim sparse-mode local-members	1454
show ip pim sparse-mode mroute detail.....	1457
show ip pim sparse-mode mroute.....	1455
show ip pim sparse-mode neighbor.....	1459
show ip pim sparse-mode nexthop.....	1461
show ip pim sparse-mode packet statistics	1462
show ip pim sparse-mode rp mapping	1464
show ip pim sparse-mode rp-hash	1463
show ip prefix-list.....	1204

show ip prefix-list.....	687
show ip protocols bgp (BGP only)	1206
show ip protocols ospf.....	820
show ip protocols rip	688
show ip resolve-via-default	631
show ip rip database.....	690
show ip rip interface	691
show ip rip	689
show ip route database	635
show ip route summary.....	637
show ip route.....	632
show ip rpf	1409
show ip sockets.....	501
show ip traffic	504
show ip-reputation categories	2709
show ip-reputation	2708
show ips categories detail.....	2618
show ips categories.....	2616
show ips.....	2615
show ipsec counters	2742
show ipsec peer	2743
show ipsec policy.....	2744
show ipsec profile	2745
show ipsec sa.....	2747
show ipv6 dhcp binding	2287
show ipv6 dhcp interface	2290
show ipv6 dhcp pool	2292
show ipv6 dhcp	2286
show ipv6 forwarding.....	614
show ipv6 interface.....	615
show ipv6 mif	1410
show ipv6 mld groups	1376
show ipv6 mld interface	1378
show ipv6 mroute	1411
show ipv6 multicast forwarding.....	1413

show ipv6 neighbors	616
show ipv6 ospf database external	892
show ipv6 ospf database grace	893
show ipv6 ospf database inter-prefix	894
show ipv6 ospf database inter-router	895
show ipv6 ospf database intra-prefix	896
show ipv6 ospf database link	897
show ipv6 ospf database network	898
show ipv6 ospf database router	900
show ipv6 ospf database	891
show ipv6 ospf interface	905
show ipv6 ospf neighbor	906
show ipv6 ospf route	907
show ipv6 ospf virtual-links	908
show ipv6 ospf	889
show ipv6 pbr route	1267
show ipv6 pim sparse-mode bsr-router	1510
show ipv6 pim sparse-mode interface detail	1513
show ipv6 pim sparse-mode interface	1511
show ipv6 pim sparse-mode local-members	1514
show ipv6 pim sparse-mode mroute detail	1517
show ipv6 pim sparse-mode mroute	1515
show ipv6 pim sparse-mode neighbor	1519
show ipv6 pim sparse-mode nexthop	1520
show ipv6 pim sparse-mode rp mapping	1523
show ipv6 pim sparse-mode rp nexthop	1524
show ipv6 pim sparse-mode rp-hash	1522
show ipv6 prefix-list	1205
show ipv6 prefix-list	717
show ipv6 protocols rip	718
show ipv6 rip database	720
show ipv6 rip interface	721
show ipv6 rip	719
show ipv6 route summary	619
show ipv6 route summary	640

show ipv6 route	617
show ipv6 route	638
show isakmp counters	2748
show isakmp key (IPsec)	2749
show isakmp peer	2750
show isakmp profile	2751
show isakmp sa	2753
show ldap server group	1659
show license external	211
show linkmon probe	1314
show linkmon probe-history	1317
show log config	368
show log permanent	370
show log	366
show mail	2367
show malware-protection	2628
show memory allocations	275
show memory history	277
show memory pools	278
show memory shared	279
show memory	273
show nat rule config-check	2605
show nat rule	2603
show nat	2602
show openvpn connections detail	2810
show openvpn connections	2809
show pbr rules brief	1274
show pbr rules brief	1324
show pbr rules	1269
show pbr rules	1319
show ping-poll	2496
show privilege	195
show process	280
show radius local-server auth-mac-promiscuous	1683
show radius local-server group	1722

show radius local-server nas	1723
show radius local-server statistics	1724
show radius local-server trustpoint	1726
show radius local-server user	1727
show radius server group	1629
show radius	1680
show reboot history	282
show resource	213
show rmon alarm	2376
show rmon event	2377
show rmon history	2379
show rmon statistics	2381
show route-map	1207
show route-map	1254
show router-id	283
show running-config antivirus	2644
show running-config atmf	2111
show running-config dpi	2697
show running-config firewall	2552
show running-config interface	156
show running-config ip-reputation	2711
show running-config ips	2620
show running-config log	372
show running-config malware-protection	2629
show running-config nat	2606
show running-config pppoe-relay	457
show running-config router ipv6 vrrp	1839
show running-config router vrrp	1840
show running-config sflow	2520
show running-config snmp	2320
show running-config snmp-discovery	2151
show running-config software-configuration	2864
show running-config ssh	2408
show running-config traffic-control	1552
show running-config trigger	2454

show running-config unencrypted	158
show running-config url-filter	2653
show running-config web-control	2676
show running-config web-redirect	235
show running-config	153
show security-password configuration	196
show security-password user	197
show sflow interface	2523
show sflow	2521
show snmp-discovery	2152
show snmp-server community	2322
show snmp-server group	2323
show snmp-server trap	2324
show snmp-server user	2325
show snmp-server view	2326
show snmp-server	2321
show software-configuration	2865
show ssh client	2412
show ssh server allow-users	2415
show ssh server deny-users	2416
show ssh server	2413
show ssh	2410
show startup-config	159
show stoat collector	2134
show stoat destinations	2136
show system mac	285
show system serialnumber	286
show system	284
show tacacs+	1811
show tech-support	287
show telnet	198
show traffic-control counters	1553
show traffic-control interface	1555
show traffic-control policy	1556
show traffic-control red-curve	1558

show traffic-control rule config-check	1560
show traffic-control rule	1561
show traffic-control	1562
show trigger	2455
show tunnel inline-processing counters	2754
show url-filter	2654
show users	199
show version	160
show vrrp (session)	1847
show vrrp counters	1843
show vrrp ipv6	1846
show vrrp	1841
show web-control bypass	2679
show web-control categories	2680
show web-control rules	2682
show web-control	2677
show web-redirect	236
shutdown (stoat-dest)	2138
shutdown	394
sid	2621
size (linkmon-probe)	1326
snmp trap link-status suppress	2328
snmp trap link-status	2327
snmp-discovery arp-polling-interval	2154
snmp-discovery community	2155
snmp-discovery deny	2156
snmp-discovery permit	2158
snmp-discovery snmp-polling-interval	2159
snmp-discovery snmp-version	2160
snmp-discovery user	2161
snmp-server community	2332
snmp-server contact	2333
snmp-server enable trap	2334
snmp-server engineID local reset	2339
snmp-server engineID local	2337

snmp-server group	2340
snmp-server host	2342
snmp-server legacy-ifadminstatus	2344
snmp-server location	2345
snmp-server source-interface	2346
snmp-server startup-trap-delay	2347
snmp-server user	2348
snmp-server view	2351
snmp-server	2330
sntp-address	2294
software-upgrade	161
software-configuration	2867
source (linkmon-probe)	1327
source-ip	2500
sport	2587
ssh client allow-legacy-ssh-rsa	2421
ssh client	2419
ssh server allow-legacy-ssh-rsa	2424
ssh server allow-users	2425
ssh server authentication	2427
ssh server deny-users	2429
ssh server max-auth-tries	2431
ssh server resolve-host	2432
ssh server scp	2433
ssh server secure-algs	2434
ssh server secure-ciphers	2435
ssh server secure-hostkey	2436
ssh server secure-kex	2437
ssh server secure-mac	2438
ssh server sftp	2439
ssh server tcpforwarding	2440
ssh server	2422
ssh	2417
state	2112
stoat collector enable	2139

stoa collector expiry-period	2140
stoa collector key	2141
stoa collector trustpoint.....	2143
stoa destination	2144
strict-user-process-control force.....	163
strict-user-process-control force.....	201
strict-user-process-control	162
strict-user-process-control	200
sub-class (htb).....	1563
sub-class (priority)	1565
sub-class (wrr)	1567
subject-name (ca-trustpoint).....	1802
subnet-mask	2229
sub-sub-class (htb).....	1569
sub-sub-class (priority).....	1571
sub-sub-class (wrr).....	1573
summary-address (IPv6 OSPF).....	909
summary-address	821
suppress-ipv4-updates.....	561
switchport atmf-agentlink	2114
switchport atmf-arealink.....	2115
switchport atmf-crosslink	2117
switchport atmf-guestlink.....	2119
switchport atmf-link	2121
synchronization	1208
tacacs-server host	1813
tacacs-server key	1815
tacacs-server timeout.....	1816
tcpdump	506
telnet server.....	203
telnet	202
terminal length.....	204
terminal monitor	289
terminal resize.....	205
test snmp trap snmp.....	2352

test	2460
time (trigger)	2461
timeout (ldap-server)	1661
timeout (ping polling)	2502
timeout (pppoe-relay)	458
timers (BGP)	1210
timers (IPv6 RIPng).....	722
timers (RIP)	692
timers spf exp (IPv6 OSPF)	911
timers spf exp	822
traceroute ipv6	620
traceroute.....	507
traffic-control enable	1575
traffic-control.....	1576
transform (IPsec Profile).....	2756
transform (ISAKMP Profile)	2758
transition-mode	1848
trap	2463
trigger activate	2465
trigger	2464
trustpoint (stoaat-dest)	2146
tunnel checksum	2787
tunnel destination (DS-Lite).....	2868
tunnel destination (GRE)	2789
tunnel destination (IPsec)	2760
tunnel destination (IPv6).....	2888
tunnel destination (L2TPv3).....	2832
tunnel df	2834
tunnel dscp	2788
tunnel dscp	2890
tunnel endpoint	2791
tunnel inline-processing	2762
tunnel local id	2835
tunnel local name (GRE).....	2793
tunnel local name (IPsec)	2763

tunnel local selector	2764
tunnel mode (IPv6)	2891
tunnel mode ds-lite	2869
tunnel mode gre multipoint	2795
tunnel mode gre	2794
tunnel mode ipsec	2766
tunnel mode l2tp v3	2836
tunnel mode lw4o6	2870
tunnel mode map-e	2871
tunnel mode openvpn tap	2811
tunnel mode openvpn tun	2812
tunnel openvpn authentication	2813
tunnel openvpn cipher	2814
tunnel openvpn expiry-bytes	2816
tunnel openvpn expiry-seconds	2817
tunnel openvpn port	2818
tunnel openvpn route	2819
tunnel openvpn tagging	2821
tunnel openvpn tls-crypt	2822
tunnel openvpn tls-version-min	2823
tunnel openvpn verify-client-certificate strict-common-name-check	2825
tunnel openvpn verify-client-certificate trustpoint	2824
tunnel oper-status-control	2767
tunnel protection ipsec (GRE)	2796
tunnel protection ipsec (IPsec)	2770
tunnel protection ipsec	2837
tunnel remote id	2838
tunnel remote name (GRE)	2797
tunnel remote name (IPsec)	2771
tunnel remote selector	2772
tunnel security-reprocessing	2774
tunnel security-reprocessing	2798
tunnel security-reprocessing	2827
tunnel security-reprocessing	2839
tunnel security-reprocessing	2872

tunnel selector paired	2775
tunnel softwire	2873
tunnel source (GRE)	2799
tunnel source (IPsec)	2776
tunnel source (IPv6)	2892
tunnel source (L2TPv3)	2840
tunnel ttl	2801
tunnel ttl	2894
type atmf guest	2122
type atmf guest	2466
type atmf node	2123
type atmf node	2467
type cpu	2469
type interface	2470
type linkmon-probe	2471
type log	2473
type memory	2474
type periodic	2475
type ping-poll	2476
type reboot	2477
type time	2478
undebg 2fa	1775
undebg aaa	1631
undebg all ipv6 pim sparse-mode	1526
undebg all pim sparse-mode	1465
undebg all	290
undebg atmf	2125
undebg bgp (BGP only)	1212
undebg ddns	562
undebg igmp	1359
undebg ip packet interface	508
undebg ipv6 ospf events	912
undebg ipv6 ospf ifsm	913
undebg ipv6 ospf lsa	914
undebg ipv6 ospf nfsm	915

undebg ipv6 ospf packet	916
undebg ipv6 ospf route.....	917
undebg ipv6 pim sparse-mode	1527
undebg ipv6 rip	723
undebg isakmp	2778
undebg mail	2368
undebg ospf events	823
undebg ospf ifsm.....	824
undebg ospf isa	825
undebg ospf nfsm.....	826
undebg ospf nsm	827
undebg ospf packet	828
undebg ospf route	829
undebg ping-poll	2504
undebg ppp	451
undebg radius	1684
undebg rip.....	694
undebg sflow	2524
undebg snmp	2353
undebg ssh client	2441
undebg ssh server.....	2442
undebg trigger.....	2479
undebg vrrp events	1851
undebg vrrp packet	1852
undebg vrrp	1850
unique-id.....	2147
up-count	2503
update now	215
update-interval (antivirus)	2645
update-interval (ddns-update-method)	563
update-interval (dpi).....	2698
update-interval (IP Reputation).....	2712
update-interval (IPS)	2622
update-interval (malware)	2630
update-interval (url-filter)	2655

update-url (ddns-update-method)	564
upstream-interface	2874
uri (download-portal)	2310
url (linkmon-probe)	1328
url-filter reload custom-lists	2657
url-filter	2658
use-ipv4-for-ipv6-updates	567
user (radsrv)	1729
username (atmf-guest)	2126
username (ddns-update-method)	568
username	206
version (ISAKMP)	2779
version (RIP)	695
virtual-ip	1853
virtual-ipv6	1855
vlan (radsrv-grp)	1731
vrrp vmac	1857
wait	376
web-categorization	2699
web-control categorize	2685
web-control	2683
web-redirect	237
whitelist (IP Reputation)	2714
whitelist (url-filter)	2659
write file	164
write memory	165
write terminal	166
zone	2589

Part 1: Setup and Troubleshooting

1

CLI Navigation Commands

Introduction

Overview This chapter provides an alphabetical reference for the commands used to navigate between different modes. This chapter also provides a reference for the help and show commands used to help navigate within the CLI.

- Command List**
- “[configure terminal](#)” on page 100
 - “[disable \(Privileged Exec mode\)](#)” on page 101
 - “[do](#)” on page 102
 - “[enable \(Privileged Exec mode\)](#)” on page 103
 - “[end](#)” on page 105
 - “[exit](#)” on page 106
 - “[help](#)” on page 107
 - “[logout](#)” on page 108
 - “[show history](#)” on page 109

configure terminal

Overview This command enters the Global Configuration command mode.

Syntax `configure terminal`

Mode Privileged Exec

Example To enter the Global Configuration command mode (note the change in the command prompt), enter the command:

```
awplus# configure terminal  
awplus(config)#
```


disable (Privileged Exec mode)

Overview This command exits the Privileged Exec mode, returning the prompt to the User Exec mode. To end a session, use the [exit](#) command.

Syntax `disable`

Mode Privileged Exec

Example To exit the Privileged Exec mode, enter the command:

```
awplus# disable
awplus>
```

Related commands

- [enable \(Privileged Exec mode\)](#)
- [end](#)
- [exit](#)

do

Overview This command lets you to run User Exec and Privileged Exec mode commands when you are in any configuration mode.

Syntax `do <command>`

Parameter	Description
<code><command></code>	Specify the command and its parameters.

Mode Any configuration mode

Example `awplus# configure terminal`
`awplus(config)# do ping 192.0.2.23`

enable (Privileged Exec mode)

Overview This command enters the Privileged Exec mode and optionally changes the privilege level for a session. If a privilege level is not specified then the maximum privilege level (15) is applied to the session. If the optional privilege level is omitted then only users with the maximum privilege level can access Privileged Exec mode without providing the password as specified by the [enable password](#) or [enable secret \(deprecated\)](#) commands. If no password is specified then only users with the maximum privilege level set with the [username](#) command can assess Privileged Exec mode.

Syntax `enable [<privilege-level>]`

Parameter	Description
<code><privilege - level></code>	Specify the privilege level for a CLI session in the range <1–15>, where 15 is the maximum privilege level, 7 is the intermediate privilege level and 1 is the minimum privilege level. The privilege level for a user must match or exceed the privilege level set for the CLI session for the user to access Privileged Exec mode. Privilege level for a user is configured by username .

Mode User Exec

Usage notes Many commands are available from the Privileged Exec mode that configure operating parameters for the device, so you should apply password protection to the Privileged Exec mode to prevent unauthorized use. Passwords can be encrypted but then cannot be recovered. Note that non-encrypted passwords are shown in plain text in configurations.

The [username](#) command sets the privilege level for the user. After login, users are given access to privilege level 1. Users access higher privilege levels with the [enable \(Privileged Exec mode\)](#) command. If the privilege level specified is higher than the users configured privilege level specified by the [username](#) command, then the user is prompted for the password for that level.

Note that a separate password can be configured for each privilege level using the [enable password](#) and the [enable secret \(deprecated\)](#) commands from the Global Configuration mode. The [service password-encryption](#) command encrypts passwords configured by the [enable password](#) and the [enable secret \(deprecated\)](#) commands, so passwords are not shown in plain text in configurations.

Example The following example shows the use of the **enable** command to enter the Privileged Exec mode (note the change in the command prompt).

```
awplus> enable
awplus#
```

The following example shows the **enable** command enabling access the Privileged Exec mode for users with a privilege level of 7 or greater. Users with a privilege level of 7 or greater do not need to enter a password to access Privileged

Exec mode. Users with a privilege level 6 or less need to enter a password to access Privilege Exec mode. Use the [enable password](#) command or the [enable secret \(deprecated\)](#) commands to set the password to enable access to Privileged Exec mode.

```
awplus> enable 7
```

```
awplus#
```

**Related
commands**

[disable \(Privileged Exec mode\)](#)

[enable password](#)

[enable secret \(deprecated\)](#)

[exit](#)

[service password-encryption](#)

[username](#)

end

Overview This command returns the prompt to the Privileged Exec command mode, from any advanced command mode.

Syntax end

Mode All advanced command modes, including Global Configuration and Interface Configuration modes.

Example The following example shows how to use the **end** command to return to the Privileged Exec mode directly from Interface Configuration mode.

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# end
awplus#
```

Related commands

- disable (Privileged Exec mode)
- enable (Privileged Exec mode)
- exit

exit

Overview This command exits the current mode, and returns the prompt to the mode at the previous level. When used in User Exec mode, the **exit** command terminates the session.

Syntax `exit`

Mode All command modes, including Interface Configuration and Global Configuration modes.

Example The following example shows the use of the **exit** command to exit Interface Configuration mode and return to Global Configuration mode.

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# exit
awplus(config)#
```

Related commands

- [disable \(Privileged Exec mode\)](#)
- [enable \(Privileged Exec mode\)](#)
- [end](#)

help

Overview This command displays a description of the AlliedWare Plus™ OS help system.

Syntax help

Mode All command modes

Example To display a description on how to use the system help, use the command:

```
awplus# help
```

Output Figure 1-1: Example output from the **help** command

```
When you need help at the command line, press '?'.

If nothing matches, the help list will be empty. Delete
characters until entering a '?' shows the available options.

Enter '?' after a complete parameter to show remaining valid
command parameters (e.g. 'show ?').

Enter '?' after part of a parameter to show parameters that
complete the typed letters (e.g. 'show ip?').
```

logout

Overview This command exits the User Exec or Privileged Exec modes and ends the session.

Syntax `logout`

Mode User Exec and Privileged Exec

Example To exit the User Exec mode, use the command:

```
awplus# logout
```


show history

Overview This command lists the commands entered in the current session. The history buffer is cleared automatically upon reboot.

The output lists all command line entries, including commands that returned an error.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show history`

Mode User Exec and Privileged Exec

Example To display the commands entered during the current session, use the command:

```
awplus# show history
```

Output Figure 1-2: Example output from the **show history** command

```
1 en
2 show ru
3 conf t
4 route-map er deny 3
5 exit
6 ex
7 di
```

2

Device GUI and Vista Manager EX Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure the Device GUI. They also allow your device to be monitored and managed by Vista Manager EX™.

For more information, see [Getting Started with the Device GUI on UTM Firewalls](#).

- Command List**
- [“atmf topology-gui enable”](#) on page 111
 - [“http log webapi-requests”](#) on page 112
 - [“http port”](#) on page 113
 - [“http secure-port”](#) on page 114
 - [“http trustpoint”](#) on page 115
 - [“log event-host”](#) on page 117
 - [“service http”](#) on page 118
 - [“show http”](#) on page 119

atmf topology-gui enable

Overview Use this command to enable the operation of Vista Manager EX on the Master device.

Vista Manager EX delivers state-of-the-art monitoring and management for your Autonomous Management Framework™ (AMF) network, by automatically creating a complete topology map of switches, firewalls and wireless access points (APs). An expanded view includes third-party devices such as security cameras.

Use the **no** variant of this command to disable operation of Vista Manager EX.

Syntax `atmf topology-gui enable`
`no atmf topology-gui enable`

Default Disabled by default on AMF Master and member nodes. Enabled by default on Controllers.

Mode Global Configuration mode

Usage notes To use Vista Manager EX, you must also enable the HTTP service on all AMF nodes, including all AMF masters and controllers. The HTTP service is enabled by default on AlliedWare Plus switches and disabled by default on AR-Series firewalls. To enable it, use the commands:

```
Node1# configure terminal
Node1(config)# service http
```

On one master in each AMF area in your network, you also need to configure the master to send event notifications to Vista Manager EX. To do this, use the commands:

```
Node1# configure terminal
Node1(config)# log event-host <ip-address> atmf-topology-event
```

Examples To enable Vista Manager EX on Node1, use the commands:

```
Node1# configure terminal
Node1(config)# atmf topology-gui enable
```

To disable Vista Manager EX on Node1, use the commands:

```
Node1# configure terminal
Node1(config)# no atmf topology-gui enable
```

Related commands [atmf enable](#)
[log event-host](#)
[service http](#)

http log webapi-requests

Overview Use this command to log authenticated web API requests. These logs allow you to monitor and debug Vista Manager EX or Device GUI interactions with your device.

See the [Logging Feature Overview and Configuration Guide](#) for more information about the different types of logging and how to filter log messages.

Use the **no** variant of this command to disable authenticated web API request logging.

Syntax `http log webapi-requests {configuration|all}`
`no http log webapi-requests`

Parameter	Description
configuration	Log PUT, POST, and DELETE requests.
all	Log PUT, POST, DELETE, and GET requests.

Default Web API request logging is disabled.

Mode Global Configuration

Example To enable logging of all authenticated web API requests, use the following commands:

```
awplus# configure terminal
awplus(config)# http log webapi-requests all
```

To disable logging of authenticated web API requests, use the following commands:

```
awplus# configure terminal
awplus(config)# no http log webapi-requests
```

Related commands [http port](#)
[service http](#)
[show log](#)

Command changes Version 5.4.8-1.1: command added

http port

Overview Use this command to change the HTTP port used to access the web-based device GUI, or to disable HTTP management.

Use the **no** variant of this command to return to using the default port, which is 80.

Syntax `http port {<1-65535>|none}`
`no http port`

Parameter	Description
<1-65535>	The HTTP port number
none	Disable HTTP management. You may want to do this if you need to use port 80 for a different service or you do not need to use HTTP at all.

Default The default port for accessing the GUI is port 80.

Mode Global Configuration

Usage notes Do not configure the HTTP port to be the same as the HTTPS port.
Note that the device will redirect from HTTP to HTTPS unless you have disabled HTTPS access, which we do not recommend doing.

Example To set the port to 8080, use the commands:

```
awplus# configure terminal
awplus(config)# http port 8080
```

To return to using the default port of 80, use the commands:

```
awplus# configure terminal
awplus(config)# no http port
```

To stop users from accessing the GUI via HTTP, use the commands:

```
awplus# configure terminal
awplus(config)# http port none
```

Related commands [http secure-port](#)
[service http](#)
[show http](#)

Command changes Version 5.4.7-2.4: command added on AR-Series devices
Version 5.4.8-0.2: command added on AlliedWare Plus switches

http secure-port

Overview Use this command to change the HTTPS port used to access the web-based device GUI, or to disable HTTPS management.

Use the **no** variant of this command to return to using the default port, which is 443.

Syntax `http secure-port {<1-65535>|none}`
`no http secure-port`

Parameter	Description
<1-65535>	The HTTPS port number
none	Disable HTTPS management. Do not do this if you want to use Vista Manager EX or the GUI.

Default The default port for accessing the GUI is port 443.

Mode Global Configuration

Usage notes Do not configure the HTTPS port to be the same as the HTTP port.
Note that if you are using Vista Manager EX and need to change the HTTPS port, you must use certificate-based authorization in Vista Manager EX. See the [Vista Manager EX Installation Guide](#) for instructions.

Example To set the port to 8443, use the commands:

```
awplus# configure terminal
awplus(config)# http secure-port 8443
```

To return to using the default port of 443, use the commands:

```
awplus# configure terminal
awplus(config)# no http secure-port
```

To stop users from accessing the GUI via HTTPS, use the commands:

```
awplus# configure terminal
awplus(config)# http secure-port none
```

Related commands [http port](#)
[service http](#)
[show http](#)

Command changes Version 5.4.7-1.1: command added on AR-Series devices
Version 5.4.7-2.4: **none** parameter added
Version 5.4.8-0.2: command added on AlliedWare Plus switches

http trustpoint

Overview Use this command to set the PKI trustpoint to use for secure HTTP communication to an AlliedWare Plus device.

Use the **no** variant of this command to revert to using the default trustpoint 'default-selfsigned'.

Syntax `http trustpoint <trustpoint-name>`
`no http trustpoint`

Parameter	Description
<code><trustpoint-name></code>	Name of trustpoint

Default By default, HTTP uses the 'default-selfsigned' trustpoint.

Mode Global Configuration

Usage notes Before using the **http trustpoint** command you will need to establish a trustpoint. For example, you can create a local self-signed trustpoint using the procedure outlined below.

Create a self-signed trustpoint called 'vista' with keypair 'vista_key':

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint vista
awplus(ca-trustpoint)# enrollment selfsigned
awplus(ca-trustpoint)# rsakeypair vista_key
awplus(ca-trustpoint)# exit
awplus(config)# exit
```

Create the root and server certificates for this trustpoint:

```
awplus# crypto pki authenticate vista
awplus# crypto pki enroll vista
```

For more information about the AlliedWare Plus implementation of Public Key Infrastructure (PKI), see the [Public Key Infrastructure \(PKI\) Feature Overview and Configuration Guide](#)

Example To configure HTTP to use the trustpoint 'vista', use the commands:

```
awplus# configure terminal
awplus(config)# http trustpoint vista
```

To configure HTTP to use the default trustpoint 'default-selfsigned', use the commands:

```
awplus# configure terminal
awplus(config)# no http trustpoint
```

**Related
commands**

[crypto pki trustpoint](#)
[show crypto pki certificates](#)
[show crypto pki trustpoint](#)

**Command
changes**

Version 5.5.1-2.1: command added

log event-host

Overview Use this command to set up an external host to log AMF topology events through Vista Manager. This command is run on the Master device.

Use the **no** variant of this command to disable log events through Vista Manager.

Syntax `log event-host [<ipv4-addr>|<ipv6-addr>] atmf-topology-event`
`no log event-host [<ipv4-addr>|<ipv6-addr>] atmf-topology-event`

Parameter	Description
<ipv4-addr>	ipv4 address of the event host
<ipv6-addr>	ipv6 address of the event host

Default Log events are disabled by default.

Mode Global Configuration

Usage notes Event hosts are set so syslog sends the messages out as they come.
Note that there is a difference between log event and log host messages:

- Log event messages are sent out as they come by syslog
- Log host messages are set to wait for a number of messages (20) to send them out together for traffic optimization.

Example To enable Node 1 to log event messages from host IP address 192.0.2.31, use the following commands:

```
Node1# configure terminal
```

```
Node1(config)# log event-host 192.0.2.31 atmf-topology-event
```

To disable Node 1 to log event messages from host IP address 192.0.2.31, use the following commands:

```
Node1# configure terminal
```

```
Node1(config)# no log event-host 192.0.2.31 atmf-topology-event
```

Related commands [atmf topology-gui enable](#)

service http

Overview Use this command to enable the HTTP (Hypertext Transfer Protocol) service. This service is required to support Vista Manager EX™ and the Device GUI. Use the **no** variant of this command to disable the HTTP feature.

Syntax `service http`
`no service http`

Default Enabled if your device came from the factory with the Device GUI pre-installed. Otherwise disabled.

Mode Global Configuration

Example To enable the HTTP service, use the following commands:

```
awplus# configure terminal
awplus(config)# service http
```

To disable the HTTP service, use the following commands:

```
awplus# configure terminal
awplus(config)# no service http
```

Related commands [http port](#)
[http secure-port](#)
[show http](#)

show http

Overview This command shows the HTTP server settings.

Syntax show http

Mode User Exec and Privileged Exec

Example To show the HTTP server settings, use the command:

```
awplus# show http
```

Output Figure 2-1: Example output from the **show http** command

```
awplus#show http
HTTP Server Configuration
-----
HTTP server           : Enabled
Port                  : 80
Secure Port           : 443

Web GUI Information
-----
GUI file in use       : -

Server Certificate
-----
Subject       : O = Allied-Telesis, CN = AlliedwarePlusCA
Issuer        : O = Allied-Telesis, CN = AlliedwarePlusCA
Valid From    : Jun  1 23:26:03 2021 GMT
Valid To      : May 30 23:26:03 2031 GMT
Fingerprints  :
  SHA-1       : 08:17:88:8C:5D:B0:D4:39:3C:8E:B6:EC:B6:BE:42:FF:57:EA:42:CC
  SHA-256     : D7:4E:D4:29:E2:DD:D0:08:F7:B1:4E:4F:47:89:09:13:47:93:B3:64:79:CC:62:E7:
  FE:A6:D8:5D:9A:9C:E5:F0
```

Related commands [clear line vty](#)
[service http](#)

3

File and Configuration Management Commands

Introduction

Overview This chapter provides an alphabetical reference of AlliedWare Plus™ OS file and configuration management commands.

Filename syntax and keyword usage Many of the commands in this chapter use the placeholder 'filename' to represent the name and location of the file that you want to act on. The following table explains the syntax of the filename for each different type of file location.

When you copy a file...	Use this syntax:	Example:
Copying in local flash memory	<code>flash: [/] [<directory> /] <filename></code>	To specify a file in the configs directory in flash: <code>flash:configs/example.cfg</code>
Copying with HTTP	<code>http:// [[<username> :<password>] @] {<hostname> <host-ip> } [/<filepath>] /<filename></code>	To specify a file in the configs directory on the server: <code>http://www.company.com/configs/example.cfg</code>
Copying with TFTP	<code>tftp:// [[<location>] /<directory>] /<filename></code>	To specify a file in the top-level directory of the server: <code>tftp://172.1.1.1/example.cfg</code>
Copying with SCP	<code>scp://<username>@<location> [/<directory>] [/<filename>]</code>	To specify a file in the configs directory on the server, logging on as user 'bob': e.g. <code>scp://bob@10.10.0.12/configs/example.cfg</code>
Copying with SFTP	<code>sftp:// [[<location>] /<directory>] /<filename></code>	To specify a file in the top-level directory of the server: <code>sftp://10.0.0.5/example.cfg</code>

Valid characters The filename and path can include characters from up to four categories. The categories are:

- 1) uppercase letters: A to Z
- 2) lowercase letters: a to z
- 3) digits: 0 to 9
- 4) special symbols: most printable ASCII characters not included in the previous three categories, including the following characters:
 - -
 - /
 - .
 - _
 - @
 - "
 - '
 - *
 - :
 - ~
 - ?

Do not use spaces, parentheses or the + symbol within filenames. Use hyphens or underscores instead.

Syntax for directory listings

A leading slash (/) indicates the root of the current file system location.

In commands where you need to specify the local file system's flash base directory, you may use **flash** or **flash:** or **flash:/**. For example, these commands are all the same:

- `dir flash`
- `dir flash:`
- `dir flash:/`

You cannot name a directory or subdirectory **flash**, **nvs**, **usb**, **card**, **tftp**, **scp**, **sftp** or **http**. These keywords are reserved for tab completion when using various file commands.

Command list

- ["boot config-file"](#) on page 123
- ["boot config-file backup"](#) on page 124
- ["boot system"](#) on page 125
- ["boot system backup"](#) on page 126
- ["cd"](#) on page 127
- ["copy \(filename\)"](#) on page 128

- [“copy debug”](#) on page 130
- [“copy running-config”](#) on page 131
- [“copy startup-config”](#) on page 132
- [“copy zmodem”](#) on page 133
- [“delete”](#) on page 134
- [“delete debug”](#) on page 135
- [“dir”](#) on page 136
- [“edit”](#) on page 138
- [“erase factory-default”](#) on page 139
- [“erase startup-config”](#) on page 140
- [“ip tftp source-interface”](#) on page 141
- [“ipv6 tftp source-interface”](#) on page 142
- [“mkdir”](#) on page 143
- [“move”](#) on page 144
- [“move debug”](#) on page 145
- [“pwd”](#) on page 146
- [“rmdir”](#) on page 147
- [“show boot”](#) on page 148
- [“show hash”](#) on page 149
- [“show file”](#) on page 150
- [“show file systems”](#) on page 151
- [“show running-config”](#) on page 153
- [“show running-config interface”](#) on page 156
- [“show running-config unencrypted”](#) on page 158
- [“show startup-config”](#) on page 159
- [“show version”](#) on page 160
- [“software-upgrade”](#) on page 161
- [“strict-user-process-control”](#) on page 162
- [“strict-user-process-control force”](#) on page 163
- [“write file”](#) on page 164
- [“write memory”](#) on page 165
- [“write terminal”](#) on page 166

boot config-file

Overview Use this command to set the configuration file to use during the next boot cycle.
Use the **no** variant of this command to remove the configuration file.

Syntax `boot config-file <filepath-filename>`
`no boot config-file`

Parameter	Description
<code><filepath-filename></code>	Filepath and name of a configuration file. The specified configuration file must exist in the specified filesystem. Valid configuration files must have a .cfg extension.

Mode Global Configuration

Usage notes For an explanation of the configuration fallback order, see the [File Management Feature Overview and Configuration Guide](#).

Examples To run the configuration file “branch.cfg” the next time the device boots up, when “branch.cfg” is stored on the device’s flash filesystem, use the commands:

```
awplus# configure terminal
awplus(config)# boot config-file flash:/branch.cfg
```

To stop running the configuration file “branch.cfg” when the device boots up, when “branch.cfg” is stored on the device’s flash filesystem, use the commands:

```
awplus# configure terminal
awplus(config)# no boot config-file flash:/branch.cfg
```

Related commands [boot config-file backup](#)
[boot system](#)
[boot system backup](#)
[show boot](#)

boot config-file backup

Overview Use this command to set a backup configuration file to use if the main configuration file cannot be accessed.

Use the **no** variant of this command to remove the backup configuration file.

Syntax `boot config-file backup <filepath-filename>`
`no boot config-file backup`

Parameter	Description
<code><filepath-filename></code>	Filepath and name of a backup configuration file. Backup configuration files must be in the flash filesystem. Valid backup configuration files must have a .cfg extension.
<code>backup</code>	The specified file is a backup configuration file.

Mode Global Configuration

Usage notes For an explanation of the configuration fallback order, see the [File Management Feature Overview and Configuration Guide](#).

Examples To set the configuration file backup.cfg as the backup to the main configuration file, use the commands:

```
awplus# configure terminal
awplus(config)# boot config-file backup flash:/backup.cfg
```

To remove the configuration file backup.cfg as the backup to the main configuration file, use the commands:

```
awplus# configure terminal
awplus(config)# no boot config-file backup flash:/backup.cfg
```

Related commands [boot config-file](#)
[boot system](#)
[boot system backup](#)
[show boot](#)

boot system

Overview Use this command to set the release file to load during the next boot cycle.

Use the **no** variant of this command to stop specifying a primary release file to boot from. If the device boots up with no release file set, it will use autoboot or the backup release file if either of those are configured. You can also use the boot menu to select a release file source. To access the boot menu, type Ctrl-B at bootup.

Syntax `boot system <filepath-filename>`
`no boot system`

Parameter	Description
<code><filepath-filename></code>	Filepath and name of a release file. The specified release file must exist and must be stored in the root directory of the specified filesystem. Valid release files must have a .rel extension.

Mode Global Configuration

Usage notes This switch stores release files in flash memory.

Examples To boot up with the release file AR4000S-Cloud-5.5.4-2.1.iso the next time the device boots up, when the release file is stored on the device's flash filesystem, use the commands:

```
awplus# configure terminal
awplus(config)# boot system flash:/AR4000S-Cloud-5.5.4-2.1.iso
```

Related commands [boot config-file](#)
[boot config-file backup](#)
[boot system backup](#)
[show boot](#)

boot system backup

Overview Use this command to set a backup release file to load if the main release file cannot be loaded.

Use the **no** variant of this command to stop specifying a backup release file.

Syntax `boot system backup <filepath-filename>`
`no boot system backup`

Parameter	Description
<code><filepath-filename></code>	Filepath and name of a backup release file. Backup release files must be in the Flash filesystem. Valid release files must have a .rel extension.
<code>backup</code>	The specified file is a backup release file.

Mode Global Configuration

Examples To specify the file AR4000S-Cloud-5.5.4-1.1.iso as the backup to the main release file, use the commands:

```
awplus# configure terminal
awplus(config)# boot system backup
flash:/AR4000S-Cloud-5.5.4-1.1.iso
```

To stop specifying a backup to the main release file, use the commands:

```
awplus# configure terminal
awplus(config)# no boot system backup
```

Related commands [boot config-file](#)
[boot config-file backup](#)
[boot system](#)
[show boot](#)

cd

Overview This command changes the current working directory.

Syntax `cd <directory-name>`

Parameter	Description
<code><directory-name></code>	Name and path of the directory.

Mode Privileged Exec

Example To change to the directory called `images`, use the command:

```
awplus# cd images
```

Related commands

- `dir`
- `pwd`
- `show file systems`

copy (filename)

Overview This command copies a file. This allows you to:

- copy files from your device to a remote device
- copy files from a remote device to your device
- create two copies of the same file on your device

Syntax `copy [force] <source-name> <destination-name>`

Parameter	Description
<code>force</code>	This parameter forces the copy command to overwrite the destination file, if it already exists, without prompting the user for confirmation.
<code><source-name></code>	The filename and path of the source file. See Introduction on page 120 for valid syntax.
<code><destination-name></code>	The filename and path for the destination file. See Introduction on page 120 for valid syntax.

Mode Privileged Exec

Examples To use TFTP to copy the file “bob.key” into the current directory from the remote server at 10.0.0.1, use the command:

```
awplus# copy tftp://10.0.0.1/bob.key bob.key
```

To use SFTP to copy the file “new.cfg” into the current directory from a remote server at 10.0.1.2, use the command:

```
awplus# copy sftp://10.0.1.2/new.cfg bob.key
```

To use SCP with the username “beth” to copy the file old.cfg into the directory config_files on a remote server that is listening on TCP port 2000, use the command:

```
awplus# copy scp://beth@serv:2000/config_files/old.cfg old.cfg
```

To copy the file “config.cfg” into the current directory from a remote file server, and rename it to “configtest.cfg”, use the command:

```
awplus# copy fserver:/config.cfg configtest.cfg
```

On an AMF network, to copy the device GUI file from the AMF master to the Flash memory of ‘node_1’, use the command:

```
master# copy awplus-gui_549_13.gui node_1.atmf/flash:
```

**Related
commands**

- [copy zmodem](#)
- [copy buffered-log](#)
- [copy permanent-log](#)
- [show file systems](#)

copy debug

Overview This command copies a specified debug file to a destination file.

Syntax `copy debug {<destination-name>|debug|flash|nvs|scp|tftp}
{<source-name>|debug|flash|nvs|scp|tftp}`

Parameter	Description
<code><destination-name></code>	The filename and path where you would like the debug output saved. See Introduction on page 120 for valid syntax.
<code><source-name></code>	The filename and path where the debug output originates. See the Introduction to this chapter for valid syntax.

Mode Privileged Exec

Example To copy debug output to a file on flash called “my-debug”, use the following command:

```
awplus# copy debug flash:my-debug
```

Output Figure 3-1: CLI prompt after entering the **copy debug** command

```
Enter source file name []:
```

Related commands [delete debug](#)
[move debug](#)

copy running-config

Overview This command copies the running-config to a destination file, or copies a source file into the running-config. Commands entered in the running-config do not survive a device reboot unless they are saved in a configuration file.

Syntax `copy <source-name> running-config`
`copy running-config [<destination-name>]`
`copy running-config startup-config`

Parameter	Description
<source-name>	The filename and path of a configuration file. This must be a valid configuration file with a .cfg filename extension. Specify this when you want the script in the file to become the new running-config. See Introduction on page 120 for valid syntax.
<destination-name>	The filename and path where you would like the current running-config saved. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See Introduction on page 120 for valid syntax. If you do not specify a file name, the device saves the running-config to a file called default.cfg.
startup-config	Copies the running-config into the file set as the current startup-config file.

Mode Privileged Exec

Examples To copy the running-config into the startup-config, use the command:

```
awplus# copy running-config startup-config
```

To copy the file 'layer3.cfg' into the running-config, use the command:

```
awplus# copy layer3.cfg running-config
```

To use SCP to copy the running-config as 'current.cfg' to the remote server listening on TCP port 2000, use the command:

```
awplus# copy running-config  
scp://user@server:2000/config_files/current.cfg
```

Related commands [copy startup-config](#)
[write file](#)
[write memory](#)

copy startup-config

Overview This command copies the startup-config script into a destination file, or alternatively copies a configuration script from a source file into the startup-config file.

Syntax `copy <source-name> startup-config`
`copy startup-config <destination-name>`

Parameter	Description
<code><source-name></code>	The filename and path of a configuration file. This must be a valid configuration file with a .cfg filename extension. Specify this to copy the script in the file into the startup-config file. Note that this does not make the copied file the new startup file, so any further changes made in the configuration file are not added to the startup-config file unless you reuse this command. See Introduction on page 120 for valid syntax.
<code><destination-name></code>	The destination and filename that you are saving the startup-config as. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See Introduction on page 120 for valid syntax.

Mode Privileged Exec

Examples To copy the file 'Layer3.cfg' to the startup-config, use the command:

```
awplus# copy Layer3.cfg startup-config
```

To copy the startup-config as the file 'oldconfig.cfg' in the current directory, use the command:

```
awplus# copy startup-config oldconfig.cfg
```

Related commands [copy running-config](#)

copy zmodem

Overview This command allows you to copy files using ZMODEM using Minicom. ZMODEM works over a serial connection and does not need any interfaces configured to do a file transfer.

Syntax `copy <source-name> zmodem`
`copy zmodem`

Parameter	Description
<code><source-name></code>	The filename and path of the source file. See Introduction on page 120 for valid syntax.

Mode Privileged Exec

Example To copy the local file 'asuka.key' using ZMODEM, use the command:

```
awplus# copy asuka.key zmodem
```

Related commands [copy \(filename\)](#)
[show file systems](#)

delete

Overview This command deletes files or directories.

Syntax delete [force] [recursive] <filename>

Parameter	Description
force	Ignore nonexistent filenames and never prompt before deletion.
recursive	Remove the contents of directories recursively.
<filename>	The filename and path of the file to delete. See Introduction on page 120 for valid syntax.

Mode Privileged Exec

Examples To delete the file `temp.cfg` from the current directory, use the command:

```
awplus# delete temp.cfg
```

To delete the read-only file `one.cfg` from the current directory, use the command:

```
awplus# delete force one.cfg
```

To delete the directory `old_configs`, which is not empty, use the command:

```
awplus# delete recursive old_configs
```

To delete the directory `new_configs`, which is not empty, without prompting if any read-only files are being deleted, use the command:

```
awplus# delete force recursive new_configs
```

Related commands [erase startup-config](#)
[rmdir](#)

delete debug

Overview Use this command to delete a specified debug output file.

Syntax `delete debug <source-name>`

Parameter	Description
<code><source-name></code>	The filename and path where the debug output originates. See Introduction on page 120 for valid URL syntax.

Mode Privileged Exec

Example To delete debug output, use the following command:

```
awplus# delete debug
```

Output Figure 3-2: CLI prompt after entering the **delete debug** command

```
Enter source file name []:
```

Related commands [copy debug](#)
[move debug](#)

dir

Overview This command lists the files on a filesystem. If you don't specify a directory or file, then this command lists the files in the current directory.

Syntax `dir [recursive] [sort [reverse] [name|size|time]]`
`[<filename>|debug|flash|nvs]`

Parameter	Description
recursive	List the contents of directories recursively.
sort	Sort directory listing.
reverse	Sort using reverse order.
name	Sort by name.
size	Sort by size.
time	Sort by modification time (default).
<filename>	The name of the directory or file. If you don't specify a directory or file, then this command lists the files in the current directory.
debug	Debug root directory.
flash	Flash memory root directory.
nvs	NVS memory root directory.

Mode Privileged Exec

Examples To list the files in the current working directory, use the command:

```
awplus# dir
```

To list the files in the root of the Flash filesystem, use the command:

```
awplus# dir flash
```

To list recursively the files in the Flash filesystem, use the command:

```
awplus# dir recursive flash:
```

To list the files in alphabetical order, use the command:

```
awplus# dir sort name
```

To list the files by size, smallest to largest, use the command:

```
awplus# dir sort reverse size
```

To sort the files by modification time, oldest to newest, use the command:

```
awplus# dir sort reverse time
```

Output Figure 3-3: Example output from the **dir** command

```
awplus#dir
      630 -rw- Nov 25 2022 23:36:31 example.cfg
23652123 -rw- Nov 25 2022 03:41:18 AR4000S-Cloud-5.5.4-2.1.iso
      149 -rw- Nov 25 2022 00:40:35 exception.log
```

**Related
commands**

- [cd](#)
- [mkdir](#)
- [pwd](#)

edit

Overview This command opens a text file in the AlliedWare Plus™ text editor. Once opened you can use the editor to alter to the file.

If you specify a filename and the file already exists, then the editor opens it in the text editor.

If you do not enter a filename, the editor opens an empty file and prompts you for a name when you exit the editor.

For information about using the editor, including control sequences, see the [File Management Feature Overview and Configuration Guide](#).

Syntax `edit [<filename>]`
`edit <remote-file>`

Parameter	Description
<code><filename></code>	The name of a file in the local Flash filesystem.
<code><remote-file></code>	The filename and path of the remote file. See Introduction on page 120 for valid syntax.

Mode Privileged Exec

Usage notes Note that files in remote filesystems cannot be edited from the text editor (e.g. files on a TFTP server). Such files will open read-only.

Before starting the editor make sure your terminal, terminal emulation program, or Telnet client is 100% compatible with a VT100 terminal. The editor uses VT100 control sequences to display text on the terminal.

Examples To create and edit a new text file, use the command:

```
awplus# edit
```

To edit the existing configuration file myconfig.cfg stored on your device's Flash memory, use the command:

```
awplus# edit myconfig.cfg
```

To view the file bob.cfg stored in configs directory of a TFTP server, use the command:

```
awplus# edit tftp://configs/bob.cfg
```

Related commands [copy \(filename\)](#)
[dir](#)
[mkdir](#)
[show file](#)

erase factory-default

Overview This command erases all data from NVS and all data from flash **except** the following:

- the boot release file (a .rel file) and its release setting file
- all license files
- the latest GUI release file

The device is then rebooted and returned to its factory default condition. The device can then be used for AMF automatic node recovery.

Syntax `erase factory-default`

Mode Privileged Exec

Usage notes This command is an alias to the [atmf cleanup](#) command.

Example To erase data, use the command:

```
Node_1# erase factory-default
```

```
This command will erase all NVS, all flash contents except for  
the boot release, a GUI resource file, and any license files,  
and then reboot the switch. Continue? (y/n):y
```

Related commands [atmf cleanup](#)

erase startup-config

Overview This command deletes the file that is set as the startup-config file, which is the configuration file that the system runs when it boots up.

At the next restart, the device loads the default configuration file, default.cfg. If default.cfg no longer exists, then the device loads with the factory default configuration. This provides a mechanism for you to return the device to the factory default settings.

Syntax `erase startup-config`

Mode Privileged Exec

Example To delete the file currently set as the startup-config, use the command:

```
awplus# erase startup-config
```

Related commands

- [boot config-file backup](#)
- [copy running-config](#)
- [copy startup-config](#)
- [show boot](#)

ip tftp source-interface

Overview Use this command to manually specify the IP address that all TFTP requests originate from. This is useful in network configurations where TFTP servers only accept requests from certain devices, or where the server cannot dynamically determine the source of the request.

Use the **no** variant of this command to stop specifying a source.

Syntax `ip tftp source-interface {<interface>|<ip-add>}`
`no ip tftp source-interface`

Parameter	Description
<interface>	The interface that TFTP requests originate from. The device will use the IP address of this interface as its source IP address. You can specify any interface that can have an IP address attached to it (e.g. a PPP or Eth interface).
<ip-add>	The IP address that TFTP requests originate from, in dotted decimal format.

Default There is no default source specified.

Mode Global Configuration

Usage This command is helpful in network configurations where TFTP traffic needs to traverse point-to-point links or subnets within your network, and you do not want to propagate those point-to-point links through your routing tables.

In those circumstances, the TFTP server cannot dynamically determine the source of the TFTP request, and therefore cannot send the requested data to the correct device. Specifying a source interface or address enables the TFTP server to send the data correctly.

Example To specify that TFTP requests originate from the IP address 192.0.2.1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip tftp source-interface 192.0.2.1
```

Related commands [copy \(filename\)](#)

ipv6 tftp source-interface

Overview Use this command to manually specify the IPv6 address that all TFTP requests originate from. This is useful in network configurations where TFTP servers only accept requests from certain devices, or where the server cannot dynamically determine the source of the request.

Use the **no** variant of this command to stop specifying a source.

Syntax `ipv6 tftp source-interface {<interface>|<ipv6-add>}`
`no ipv6 tftp source-interface`

Parameter	Description
<interface>	The interface that TFTP requests originate from. The device will use the IPv6 address of this interface as its source IPv6 address. You can specify any interface that can have an IPv6 address attached to it (e.g. a PPP or Eth interface).
<ipv6-add>	The IPv6 address that TFTP requests originate from, in the format x:x::x:x, for example, 2001:db8::8a2e:7334.

Default There is no default source specified.

Mode Global Configuration

Usage This command is helpful in network configurations where TFTP traffic needs to traverse point-to-point links or subnets within your network, and you do not want to propagate those point-to-point links through your routing tables.

In those circumstances, the TFTP server cannot dynamically determine the source of the TFTP request, and therefore cannot send the requested data to the correct device. Specifying a source interface or address enables the TFTP server to send the data correctly.

Example To specify that TFTP requests originate from the IPv6 address 2001:db8::8a2e:7334, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 tftp source-interface 2001:db8::8a2e:7334
```

Related commands [copy \(filename\)](#)

mkdir

Overview This command makes a new directory.

Syntax `mkdir <name>`

Parameter	Description
<code><name></code>	The name and path of the directory that you are creating.

Mode Privileged Exec

Usage You cannot name a directory or subdirectory **flash**, **nvs**, **usb**, **card**, **tftp**, **scp**, **sftp** or **http**. These keywords are reserved for tab completion when using various file commands.

Example To make a new directory called `images` in the current directory, use the command:

```
awplus# mkdir images
```

Related commands `cd`
`dir`
`pwd`

move

Overview This command renames or moves a file.

Syntax `move <source-name> <destination-name>`

Parameter	Description
<code><source-name></code>	The filename and path of the source file. See Introduction on page 120 for valid syntax.
<code><destination-name></code>	The filename and path of the destination file. See Introduction on page 120 for valid syntax.

Mode Privileged Exec

Examples To rename the file `temp.cfg` to `startup.cfg`, use the command:

```
awplus# move temp.cfg startup.cfg
```

To move the file `temp.cfg` from the root of the Flash filesystem to the directory `myconfigs`, use the command:

```
awplus# move temp.cfg myconfigs/temp.cfg
```

Related commands

- [delete](#)
- [edit](#)
- [show file](#)
- [show file systems](#)

move debug

Overview This command moves a specified debug file to a destination debug file.

Syntax `move debug {<destination-name>|debug|nvs|flash}`

Parameter	Description
<code><destination-name></code>	The filename and path where you would like the debug output moved to. See Introduction on page 120 for valid syntax.

Mode Privileged Exec

Example To move debug output into Flash memory with a filename “my-debug”, use the following command:

```
awplus# move debug flash:my-debug
```

Output Figure 3-4: CLI prompt after entering the **move debug** command

```
Enter source file name []:
```

Related commands [copy debug](#)
[delete debug](#)

pwd

Overview This command prints the current working directory.

Syntax `pwd`

Mode Privileged Exec

Example To print the current working directory, use the command:

```
awplus# pwd
```

**Related
commands** `cd`

rmkdir

Overview This command removes a directory. This command only works on empty directories, unless you specify the optional **force** keyword.

Syntax `rmkdir [force] <name>`

Parameter	Description
<code>force</code>	Optional keyword that allows you to delete directories that are not empty and contain files or subdirectories.
<code><name></code>	The name and path of the directory.

Mode Privileged Exec

Usage notes You can use the CLI to access filesystems on a specific external memory device. See the [Introduction](#) on page 120 for syntax details.

Examples To remove the directory “images” from the top level of the Flash filesystem, use the command:

```
awplus# rmkdir flash:/images
```

To create a directory called “level1” containing a subdirectory called “level2”, and then force the removal of both directories, use the commands:

```
awplus# mkdir level1
awplus# mkdir level1/level2
awplus# rmkdir force level1
```

Related commands [cd](#)
[dir](#)
[mkdir](#)
[pwd](#)

show boot

Overview This command displays the current boot configuration.

Syntax show boot

Mode Privileged Exec

Example To show the current boot configuration, use the command:

```
awplus# show boot
```

Output Figure 3-5: Example output from **show boot**

```
awplus#show boot
Boot configuration
-----
Current software   : AR4000S-Cloud-5.5.4-2.1.iso
Current boot image : flash:/AR4000S-Cloud-5.5.4-2.1.iso
Backup boot image  : flash:/AR4000S-Cloud-5.5.4-1.1.iso
Default boot config: flash:/default.cfg
Current boot config: flash:/my.cfg (file exists)
Backup boot config: flash:/backup.cfg (file not found)
Autoboot status    : disabled
```

Table 3-1: Parameters in the output from **show boot**

Parameter	Description
Current software	The current software release that the device is using.
Default boot config	The default startup configuration file. The device loads this configuration script if no file is set as the startup-config file.
Current boot config	The configuration file currently configured as the startup-config file. The device loads this configuration file during the next boot cycle if this file exists.
Backup boot config	The configuration file to use during the next boot cycle if the main configuration file cannot be loaded.
Autoboot status	The status of the Autoboot feature; either enabled or disabled.

Related commands [boot config-file backup](#)

show hash

Overview Use this command to display the hash for a specified file on the device.

Syntax `show hash <filename>`

Parameter	Description
<filename>	The name of the file to display the hash for.

Mode Privileged Exec

Examples To show the hash for the GUI file named `awplus-gui_552_27.gui`, use the command:

```
awplus# show hash awplus-gui_552_27.gui
```

To show the hash for a file named 'example.txt', which is in the folder named 'example' in flash memory, use the command:

```
awplus# show hash flash://example/example.txt
```

Output Figure 3-6: Example output from **show hash**

```
awplus#show hash awplus-gui_552_27.gui
b793e2c7fc5580513472017f964316f3bb0e79fbf1ddfd6f3844a2a8311c5c64
```

Command changes Version 5.5.3-0.1: command added

show file

Overview This command displays the contents of a specified file.

Syntax `show file <filename>`

Parameter	Description
<code><filename></code>	Name of a file on the local Flash filesystem, or name and directory path of a file.

Mode Privileged Exec

Example To display the contents of the file `oldconfig.cfg`, which is in the current directory, use the command:

```
awplus# show file oldconfig.cfg
```

Related commands [edit](#)
[show file systems](#)

show file systems

Overview This command lists the file systems and their utilization information where appropriate.

Syntax show file systems

Mode Privileged Exec

Examples To display the file systems, use the command:

```
awplus# show file systems
```

Output Figure 3-7: Example output from the **show file systems** command

awplus#show file systems							
Size (b)	Free (b)	Type	Flags	Prefixes	S/D/V	Lcl/Ntwk	Avail
968.3M	882.3M	flash	rw	flash:	static	local	Y
-	-	system	rw	system:	virtual	local	-
10.0M	9.9M	debug	rw	debug:	static	local	Y
-	-	fserver	rw	fserver:	dynamic	network	N
-	-	tftp	rw	tftp:	-	network	-
-	-	scp	rw	scp:	-	network	-
-	-	sftp	ro	sftp:	-	network	-
-	-	http	ro	http:	-	network	-
-	-	rsync	rw	rsync:	-	network	-

Table 4: Parameters in the output of the **show file systems** command

Parameter	Description
Size (b)	The total memory available to this file system. The units are given after the value and are M for Megabytes or K for kilobytes.
Free (b)	The total memory free within this file system. The units are given after the value and are M for Megabytes or K for kilobytes.
Type	The memory type used for this file system, such as: flash system tftp scp sftp http.
Flags	The file setting options: rw (read write), ro (read only).

Table 4: Parameters in the output of the **show file systems** command (cont.)

Parameter	Description
Prefixes	The prefixes used when entering commands to access the file systems, such as: flash system tftp scp sftp http.
S/D/V	The memory type: Static, Dynamic, Virtual.
Lcl / Ntwk	Whether the memory is located locally or via a network connection.
Avail	Whether the memory is accessible: Y (yes), N (no), - (not applicable)

**Related
commands** [edit](#)
[show file](#)

show running-config

Overview This command displays the current configuration of your device. Its output includes all non-default configuration. The default settings are not displayed.

NOTE: You can control the output by entering `|` or `>` at the end of the command:

- To display only lines that contain a particular word, enter:
`| include <word>`
- To start the display at the first line that contains a particular word, enter:
`| begin <word>`
- To save the output to a file, enter:
`> <filename>`

Syntax `show running-config [full|<feature>]`

Parameter	Description																												
full	Display the running-config for all features. This is the default setting, so it is the same as entering show running-config .																												
<feature>	Display only the configuration for a single feature. The features available depend on your device and will be some of the following list: <table><tr><td>access-list</td><td>ACL configuration</td></tr><tr><td>antivirus</td><td>Antivirus configuration</td></tr><tr><td>application</td><td>Application configuration</td></tr><tr><td>as-path</td><td>Autonomous system path filter configuration</td></tr><tr><td>as-path access-list</td><td>Configuration of ACLs for AS path filtering</td></tr><tr><td>atmf</td><td>Allied Telesis Management Framework configuration</td></tr><tr><td>bgp</td><td>Border Gateway Protocol (BGP) configuration</td></tr><tr><td>community-list</td><td>Community-list configuration</td></tr><tr><td>crypto</td><td>Security-specific configuration</td></tr><tr><td>dhcp</td><td>DHCP configuration</td></tr><tr><td>dpi</td><td>Deep Packet Inspection configuration</td></tr><tr><td>entity</td><td>Entity configuration</td></tr><tr><td>firewall</td><td>Firewall configuration</td></tr><tr><td>interface</td><td>Interface configuration. See show running-config interface for further options.</td></tr></table>	access-list	ACL configuration	antivirus	Antivirus configuration	application	Application configuration	as-path	Autonomous system path filter configuration	as-path access-list	Configuration of ACLs for AS path filtering	atmf	Allied Telesis Management Framework configuration	bgp	Border Gateway Protocol (BGP) configuration	community-list	Community-list configuration	crypto	Security-specific configuration	dhcp	DHCP configuration	dpi	Deep Packet Inspection configuration	entity	Entity configuration	firewall	Firewall configuration	interface	Interface configuration. See show running-config interface for further options.
access-list	ACL configuration																												
antivirus	Antivirus configuration																												
application	Application configuration																												
as-path	Autonomous system path filter configuration																												
as-path access-list	Configuration of ACLs for AS path filtering																												
atmf	Allied Telesis Management Framework configuration																												
bgp	Border Gateway Protocol (BGP) configuration																												
community-list	Community-list configuration																												
crypto	Security-specific configuration																												
dhcp	DHCP configuration																												
dpi	Deep Packet Inspection configuration																												
entity	Entity configuration																												
firewall	Firewall configuration																												
interface	Interface configuration. See show running-config interface for further options.																												

Parameter	Description
ip	Internet Protocol (IP) configuration
ip pim dense-mode	PIM-DM configuration
ip pim sparse-mode	PIM-SM configuration
ip route	IP static route configuration
ip-reputation	IP Reputation configuration
ips	IPS configuration
ipsec	Internet Protocol Security (IPsec) configuration
ipv6	Internet Protocol version 6 (IPv6) configuration
ipv6 access-list	IPv6 ACL configuration
ipv6 mroute	IPv6 multicast route configuration
ipv6 prefix-list	IPv6 prefix list configuration
ipv6 route	IPv6 static route configuration
isakmp	Internet Security Association Key Management Protocol (ISAKMP) configuration
key chain	Authentication key management configuration
l2tp-profile	L2TP tunnel profile configuration
lldp	LLDP configuration
log	Logging utility configuration
malware-protection	Malware protection configuration
nat	Network Address Translation configuration
power-inline	Power over Ethernet (PoE) configuration
policy-based-routing	Policy-based routing (PBR) configuration
pppoe-ac	PPPoE access concentrator configuration
prefix-list	Prefix-list configuration
route-map	Route-map configuration
router	Router configuration
router-id	Configuration of the router identifier for this system
security-password	Strong password security configuration
snmp	SNMP configuration
ssh	Secure Shell configuration

Parameter	Description
switch	Switch configuration
web-control	Web Control configuration

Mode Privileged Exec and Global Configuration

Example To display the current configuration of your device, use the command:

```
awplus# show running-config
```

Output Figure 3-8: Example output from **show running-config**

```
awplus#show running-config
!
service password-encryption
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
service ssh
!
no service telnet
!
service http
!
no clock timezone

...

line con 0
line vty 0 4
!
end
```

Related commands

- [copy running-config](#)
- [show running-config interface](#)
- [show running-config unencrypted](#)

show running-config interface

Overview This command displays the current configuration of one or more interfaces on the device.

You can optionally limit the command output to display only information for a given protocol or feature. The features available depend on your device and will be a subset of the features listed in the table below.

Syntax

```
show running-config interface
show running-config interface <interface-list>
show running-config interface <interface-list> <feature>
show running-config interface <interface-list> ip <feature>
show running-config interface <interface-list> ipv6 <feature>
```

Parameter	Description
<interface-list>	The interfaces or ports to display information about. An interface-list can be: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. The specified interfaces must exist.
cfm	Displays running configuration for CFM (Connectivity Fault Management) for the specified interfaces.
dot1x	Displays running configuration for 802.1X port authentication for the specified interfaces.
lacp	Displays running configuration for LACP (Link Aggregation Control Protocol) for the specified interfaces.
ip igmp	Displays running configuration for IGMP (Internet Group Management Protocol) for the specified interfaces.
ip multicast	Displays running configuration for general multicast settings for the specified interfaces.
ip pim sparse-mode	Displays running configuration for PIM-SM (Protocol Independent Multicast - Sparse Mode) for the specified interfaces.

Parameter	Description
ip pim dense-mode	Displays running configuration for PIM-DM (Protocol Independent Multicasting - Dense Mode) for the specified interfaces.
mstp	Displays running configuration for MSTP (Multiple Spanning Tree Protocol) for the specified interfaces.
ospf	Displays running configuration for OSPF (Open Shortest Path First) for the specified interfaces.
rip	Displays running configuration for RIP (Routing Information Protocol) for the specified interfaces.
ipv6 rip	Displays running configuration for RIPng (RIP for IPv6) for the specified interfaces.
ipv6 ospf	Displays running configuration for IPv6 OSPF (Open Shortest Path First) for the specified interfaces.
ipv6 pim sparse-mode	Displays running configuration for PIM-SM (Protocol Independent Multicast - Sparse Mode) for the specified interfaces.
rstp	Displays running configuration for RSTP (Rapid Spanning Tree Protocol) for the specified interfaces.
stp	Displays running configuration for STP (Spanning Tree Protocol) for the specified interfaces.

Mode Privileged Exec and Global Configuration

Default Displays information for all protocols on all interfaces

Examples To display the current running configuration of your device for eth0, use the command:

```
awplus# show running-config interface eth0
```

To display the current OSPF configuration of your device for eth1, use the command:

```
awplus# show running-config interface eth1 ospf
```

Output Figure 3-9: Example output from a **show running-config interface ppp0** command

```
awplus#show running-config interface ppp0
!
interface ppp0
  ipv6 address 2001:db9::a3/64
  ipv6 enable
  snmp trap link-status
!
```

Related commands [copy running-config](#)
[show running-config](#)

show running-config unencrypted

Overview Use this command to display the running configuration, with passwords in cleartext (unencrypted). Otherwise passwords are displayed in encrypted form. For security reasons, use this command with caution.

This command can only be entered by users who have a privilege level of 15.

Syntax `show running-config unencrypted`

Mode Privileged Exec

Example To display the running configuration with unencrypted passwords, use the command:

```
awplus# show running-config unencrypted
```

Related commands [show running-config](#)

Command changes Version 5.5.3-2.1: command added

show startup-config

Overview This command displays the contents of the start-up configuration file, which is the file that the device runs on start-up.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show startup-config`

Mode Privileged Exec

Example To display the contents of the current start-up configuration file, use the command:

```
awplus# show startup-config
```

Output Figure 3-10: Example output from the **show startup-config** command

```
awplus#show startup-config
!
service password-encryption
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
service ssh
!
no service telnet
!
service http
!
no clock timezone

...

line con 0
line vty 0 4
!
end
```

Related commands

- [boot config-file backup](#)
- [copy running-config](#)
- [copy startup-config](#)
- [erase startup-config](#)
- [show boot](#)

show version

Overview This command displays the version number and copyright details of the current AlliedWare Plus™ OS your device is running.

Syntax `show version`

Mode User Exec and Privileged Exec

Example To display the version details of your currently installed software, use the command:

```
awplus# show version
```

Related commands [boot system backup](#)
[show boot](#)

software-upgrade

Overview Use this command to update the firmware on your Virtual UTM Firewall installation.

Syntax `software-upgrade <filename>`

Parameter	Description
<code><filename></code>	The name of the firmware file (ISO image file).

Mode Privileged Exec

Usage Notes Make sure you copy the ISO image for the new version to your Virtual UTM Firewall installation before running this command.

This command only works if your Virtual UTM Firewall ISO image is attached as a virtual hard drive on your virtual machine.

You will see the following message if this command is not suitable for your installation:

```
% Software upgrade not applicable to this device.
```

Example To update your firmware to AR4000S-Cloud-5.5.4-2.1.iso:

1) Make sure the ISO image file exists on the file system.

```
awplus# dir
```

```
...  
25499648 -rw- Jul 16 2022 20:45:45 5.5.4  
...
```

2) Upgrade the software and enter “y” at the prompt.

```
awplus# software-upgrade AR4000S-Cloud-5.5.4-2.1.iso
```

```
Install this release to disk? (y/n): y  
Upgrade succeeded, the changes will take effect after rebooting  
the device.
```

3) Reboot with the new firmware.

```
awplus# reboot
```

Related commands [show boot](#)

strict-user-process-control

Overview Use this command to enable Strict User Process Control.

Strict User Process Control protects sensitive system resources from modification. It does this by preventing use of:

- some file and directory manipulation commands
- trigger scripting commands
- the **erase factory-default** command.

Use the **no** variant of this command to turn off Strict User Process Control.

Syntax `strict-user-process-control`
`no strict-user-process-control`

Default Disabled.

Mode Global Configuration

Usage notes When you enter the **strict-user-process-control** command, it prompts you for a password. Make the password different from any existing privileged management passwords. Store the password carefully and securely, because you will need it if you want to disable the feature.

In addition, the device will prompt you to save your configuration and reboot. This ensures the change takes effect correctly.

The command must be entered from a physical console; entering it from a remote login session is not allowed for extra security.

You can use the **show running-config** command to confirm whether Strict User Process Control is on or off. If the feature is running the output will contain the command **strict-user-process-control**.

Example To protect sensitive system files from access, use the commands:

```
awplus# configure terminal
awplus(config)# strict-user-process-control
```

Related commands [show running-config](#)
[strict-user-process-control force](#)

Command changes Version 5.5.2-2.1: command added

strict-user-process-control force

Overview Use this command to enable Strict User Process Control permanently, in a way that means it can never be disabled.

Strict User Process Control protects sensitive system resources from modification. It does this by preventing use of:

- some file and directory manipulation commands
- trigger scripting commands
- the **erase factory-default** command.

CAUTION: Only use this command if you have to do so for compliance with specific security certifications. Once you have turned this feature on, you will not be able to remove it.

Syntax `strict-user-process-control force`

Default Disabled.

Mode Global Configuration

Usage notes When you enter this command, the device will prompt you to save your configuration and reboot. This ensures the change takes effect correctly.

Unlike the **strict-user-process-control** command, this **strict-user-process-control force** command enables Strict User Process Control without prompting for or saving a password. This means you cannot disable Strict User Process Control using the **no** variant of the command (or in any other way).

The command must be entered from a physical console; entering it from a remote login session is not allowed for extra security.

You can use the **show running-config** command to confirm whether Strict User Process Control is on or off.

Example To permanently protect sensitive system files from access, use the commands:

```
awplus# configure terminal
awplus(config)# strict-user-process-control force
```

Related commands [show running-config](#)
[strict-user-process-control](#)

Command changes Version 5.5.4-1.8: command added

write file

Overview This command copies the running-config into the file that is set as the current startup-config file. This command is a synonym of the **write memory** and **copy running-config startup-config** commands.

Syntax write [file]

Mode Privileged Exec

Example To write configuration data to the start-up configuration file, use the command:
`awplus# write file`

Related commands

- [copy running-config](#)
- [write memory](#)
- [show running-config](#)

write memory

Overview This command copies the running-config into the file that is set as the current startup-config file. This command is a synonym of the **write file** and **copy running-config startup-config** commands.

Syntax write [memory]

Mode Privileged Exec

Example To write configuration data to the start-up configuration file, use the command:

```
awplus# write memory
```

Related commands

- [copy running-config](#)
- [write file](#)
- [show running-config](#)

write terminal

Overview This command displays the current configuration of the device. This command is a synonym of the [show running-config](#) command.

Syntax write terminal

Mode Privileged Exec

Example To display the current configuration of your device, use the command:

```
awplus# write terminal
```

Related commands [show running-config](#)

4

User Access Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure user access.

- Command List**
- [“aaa authentication enable default local”](#) on page 169
 - [“aaa local authentication attempts lockout-time”](#) on page 170
 - [“aaa local authentication attempts max-fail”](#) on page 171
 - [“aaa login fail-delay”](#) on page 172
 - [“clear aaa local user lockout”](#) on page 173
 - [“clear line vty”](#) on page 174
 - [“enable password”](#) on page 175
 - [“enable secret \(deprecated\)”](#) on page 177
 - [“exec-timeout”](#) on page 178
 - [“length \(asyn\)”](#) on page 179
 - [“line”](#) on page 180
 - [“privilege level”](#) on page 181
 - [“security-password history”](#) on page 182
 - [“security-password forced-change”](#) on page 183
 - [“security-password lifetime”](#) on page 184
 - [“security-password min-lifetime-enforce”](#) on page 185
 - [“security-password minimum-categories”](#) on page 186
 - [“security-password minimum-length”](#) on page 187
 - [“security-password reject-expired-pwd”](#) on page 188
 - [“security-password warning”](#) on page 189

- ["service advanced-vty"](#) on page 190
- ["service password-encryption"](#) on page 191
- ["service telnet"](#) on page 192
- ["show aaa local user locked"](#) on page 193
- ["show privilege"](#) on page 195
- ["show security-password configuration"](#) on page 196
- ["show security-password user"](#) on page 197
- ["show telnet"](#) on page 198
- ["show users"](#) on page 199
- ["strict-user-process-control"](#) on page 200
- ["strict-user-process-control force"](#) on page 201
- ["telnet"](#) on page 202
- ["telnet server"](#) on page 203
- ["terminal length"](#) on page 204
- ["terminal resize"](#) on page 205
- ["username"](#) on page 206

aaa authentication enable default local

Overview This command enables local privilege level authentication.
Use the **no** variant of this command to disable local privilege level authentication.

Syntax `aaa authentication enable default local`
`no aaa authentication enable default`

Default Local privilege level authentication is enabled by default.

Mode Global Configuration

Usage notes The privilege level configured for a particular user in the local user database is the privilege threshold above which the user is prompted for an [enable \(Privileged Exec mode\)](#) command.

Examples To enable local privilege level authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default local
```

To disable local privilege level authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication enable default
```

Related commands [aaa authentication login](#)
[enable \(Privileged Exec mode\)](#)
[enable password](#)
[enable secret \(deprecated\)](#)

aaa local authentication attempts lockout-time

Overview This command configures the duration of the user lockout period.

Use the **no** variant of this command to restore the duration of the user lockout period to its default of 300 seconds (5 minutes).

Syntax `aaa local authentication attempts lockout-time <lockout-time>`
`no aaa local authentication attempts lockout-time`

Parameter	Description
<code><lockout-time></code>	<code><0-10000></code> . Time in seconds to lockout the user.

Mode Global Configuration

Default The default for the lockout-time is 300 seconds (5 minutes).

Usage notes While locked out all attempts to login with the locked account will fail. The lockout can be manually cleared by another privileged account using the [clear aaa local user lockout](#) command.

Examples To configure the lockout period to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts lockout-time
600
```

To restore the default lockout period of 5 minutes (300 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# no aaa local authentication attempts
lockout-time
```

Related commands [aaa local authentication attempts max-fail](#)
[aaa local authentication attempts max-fail remote-login-only](#)
[clear aaa local user lockout](#)

aaa local authentication attempts max-fail

Overview This command configures the maximum number of failed login attempts before a user account is locked out. Every time a login attempt fails the failed login counter is incremented.

Use the **no** variant of this command to restore the maximum number of failed login attempts to the default setting (five failed login attempts).

Syntax `aaa local authentication attempts max-fail <failed-logins>`
`no aaa local authentication attempts max-fail`

Parameter	Description
<code><failed-logins></code>	<code><1-32></code> . Number of login failures allowed before locking out a user.

Mode Global Configuration

Default The default for the maximum number of failed login attempts is five failed login attempts.

Usage When the failed login counter reaches the limit configured by this command that user account is locked out for a specified duration configured by the [aaa local authentication attempts lockout-time](#) command.

When a successful login occurs the failed login counter is reset to 0. When a user account is locked out all attempts to login using that user account will fail.

Examples To configure the number of login failures that will lock out a user account to two login attempts, use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts max-fail 2
```

To restore the number of login failures that will lock out a user account to the default number of login attempts (five login attempts), use the commands:

```
awplus# configure terminal
awplus(config)# no aaa local authentication attempts max-fail
```

Related commands [aaa local authentication attempts lockout-time](#)
[aaa local authentication attempts max-fail remote-login-only](#)
[clear aaa local user lockout](#)

aaa login fail-delay

Overview Use this command to configure the minimum time period between failed login attempts. This setting applies to login attempts via the console, SSH and Telnet. Use the **no** variant of this command to reset the minimum time period to its default value.

Syntax `aaa login fail-delay <1-10>`
`no aaa login fail-delay`

Parameter	Description
<1-10>	The minimum number of seconds required between login attempts

Default 1 second

Mode Global configuration

Example To apply a delay of at least 5 seconds between login attempts, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa login fail-delay 5
```

Related commands [aaa authentication login](#)
[aaa local authentication attempts logout-time](#)
[clear aaa local user logout](#)

clear aaa local user lockout

Overview Use this command to clear the lockout on a specific user account or all user accounts.

Syntax `clear aaa local user lockout {username <username>|all}`

Parameter	Description
username	Clear lockout for the specified user.
<username>	Specifies the user account.
all	Clear lockout for all user accounts.

Mode Privileged Exec

Examples To unlock the user account 'bob' use the following command:

```
awplus# clear aaa local user lockout username bob
```

To unlock all user accounts use the following command:

```
awplus# clear aaa local user lockout all
```

Related commands [aaa local authentication attempts lockout-time](#)

clear line vty

Overview This command resets a VTY line. If a session exists on the line then it is closed.

Syntax `clear line vty <0-32>`

Parameter	Description
<0-32>	Line number

Mode Privileged Exec

Example To reset the first VTY line, use the command:

```
awplus# clear line vty 1
```

Related commands

- [privilege level](#)
- [line](#)
- [show telnet](#)
- [show users](#)

enable password

Overview Use this command to set a local password to control access to elevated privilege levels.

Use the **no** version of the command to remove the password.

Note that the [enable secret \(deprecated\)](#) command is an outdated alias for the **enable password** command.

Syntax

```
enable password [8] <password>  
enable password level <1-15> [8] <password>  
no enable password [level <1-15>]
```

Parameter	Description
<password>	The password. The password can be up to 32 characters in length and include characters from up to four categories. The password categories are: - uppercase letters: A to Z - lowercase letters: a to z - digits: 0 to 9 - special symbols: all printable ASCII characters not included in the previous three categories. The question mark ? cannot be used as it is reserved for help functionality.
8	The parameter 8 means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form. Note that the user needs to enter the plain-text version of the password when logging in.
level	Privilege level <1-15>. Level for which the password applies. You can specify up to 16 privilege levels, using numbers 1 through 15. Level 1 is normal EXEC-mode user privileges for User Exec mode. If this argument is not specified in the command or the no variant of the command, the privilege level defaults to 15 (enable mode privileges) for Privileged Exec mode. A privilege level of 7 can be set for intermediate CLI security.

Default Level 15

Mode Global Configuration

Usage notes This command enables the Network Administrator to set a password for entering the Privileged Exec mode when using the [enable \(Privileged Exec mode\)](#) command.

You can use this command to give a user an intermediate CLI security level (privilege level 7). Such users can access all the show commands in Privileged Exec mode and all the commands in User Exec mode, but not any configuration commands in Privileged Exec mode.

The device stores passwords in hashed form in configuration files, unless you disable [service password-encryption](#).

**Related
commands**

[enable \(Privileged Exec mode\)](#)

[enable secret \(deprecated\)](#)

[service password-encryption](#)

[privilege level](#)

[show privilege](#)

[username](#)

[show running-config](#)

enable secret (deprecated)

Overview This command has been deprecated. It has been replaced by the [enable password](#) command.

exec-timeout

Overview This command sets the interval your device waits for user input from either a console or VTY connection. Once the timeout interval is reached, the connection is dropped. This command sets the time limit when the console or VTY connection automatically logs off after no activity.

The **no** variant of this command removes a specified timeout and resets to the default timeout (10 minutes).

Syntax `exec-timeout {<minutes>} [<seconds>]`
`no exec-timeout`

Parameter	Description
<minutes>	<0-35791> Required integer timeout value in minutes
<seconds>	<0-2147483> Optional integer timeout value in seconds

Default The default for the **exec-timeout** command is 10 minutes and 0 seconds (**exec-timeout 10 0**).

Mode Line Configuration

Usage notes This command is used set the time the telnet session waits for an idle VTY session, before it times out. An **exec-timeout 0 0** setting will cause the telnet session to wait indefinitely. The command **exec-timeout 0 0** is useful while configuring a device, but reduces device security.

If no input is detected during the interval then the current connection resumes. If no connections exist then the terminal returns to an idle state and disconnects incoming sessions.

Examples To set VTY connections to timeout after 2 minutes, 30 seconds if there is no response from the user, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)# exec-timeout 2 30
```

Related commands [line](#)
[service telnet](#)
[show running-config](#)

length (asyn)

Overview Use this command to specify the number of rows of output that the device will display before pausing, for the console or VTY line that you are configuring.

The **no** variant of this command restores the length of a line (terminal session) attached to a console port or to a VTY to its default length of 22 rows.

Syntax `length <0-512>`
`no length`

Parameter	Description
<0-512>	Number of lines on screen. Specify 0 for no pausing.

Mode Line Configuration

Default The length of a terminal session is 22 rows. The **no length** command restores the default.

Usage notes If the output from a command is longer than the length of the line the output will be paused and the '–More–' prompt allows you to move to the next screen full of data.

A length of 0 will turn off pausing and data will be displayed to the console as long as there is data to display.

Examples To set the terminal session length on VTY 4 to 10 rows, use the commands:

```
awplus# configure terminal
awplus(config)# line vty 0 4
awplus(config-line)# length 10
```

To reset the terminal session length on VTY 4 to the default (22 rows), use the commands:

```
awplus# configure terminal
awplus(config)# line vty 0 4
awplus(config-line)# no length
```

To display output to VTY 4 continuously, use the commands:

```
awplus# configure terminal
awplus(config)# line vty 0 4
awplus(config-line)# length 0
```

Related commands [terminal resize](#)
[terminal length](#)

line

Overview Use this command to enter line configuration mode for the specified VTYS or the console. The command prompt changes to show that the device is in Line Configuration mode.

Syntax `line vty <first-line> [<last-line>]`

Parameter	Description
<first-line>	<0-32> Specify the first line number.
<last-line>	<0-32> Specify the last line number.
vtty	Virtual terminal for remote console access.

Mode Global Configuration

Usage notes This command puts you into Line Configuration mode. Once in Line Configuration mode, you can configure console and virtual terminal settings, including setting [length \(asyn\)](#), [privilege level](#), and authentication ([login authentication](#)) or accounting ([accounting login](#)) method lists.

Note that line configuration commands do not take effect immediately. Line configuration commands take effect after one of the following commands or events:

- issuing a [clear line console](#) command
- issuing a [reboot](#) command
- logging out of the current session

Examples To enter Line Configuration mode in order to configure all VTYS, use the commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)#
```

Related commands

- [accounting login](#)
- [clear line vty](#)
- [length \(asyn\)](#)
- [login authentication](#)
- [privilege level](#)

privilege level

Overview This command sets a privilege level for VTY or console connections. The configured privilege level from this command overrides a specific user's initial privilege level at the console login.

Syntax `privilege level <1-15>`

Mode Line Configuration

Usage notes You can set an intermediate CLI security level for a console user with this command by applying privilege level 7 to access all show commands in Privileged Exec and all User Exec commands. However, intermediate CLI security will not show configuration commands in Privileged Exec.

Examples To set all VTY connections to have the maximum privilege level, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# privilege level 15
```

To set all VTY connections to have the minimum privilege level, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# privilege level 1
```

To set all VTY connections to have an intermediate CLI security level, to access all show commands, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# privilege level 7
```

Related commands

- [enable password](#)
- [line](#)
- [show privilege](#)
- [username](#)

security-password history

Overview This command specifies the number of previous passwords that are unable to be reused. A new password is invalid if it matches a password retained in the password history.

The **no** variant of the command disables this feature.

Syntax `security-password history <0-15>`
`no security-password history`

Parameter	Description
<0-15>	The allowable range of previous passwords to match against. A value of 0 will disable the history functionality and is equivalent to the no security-password history command. If the history functionality is disabled, all users' password history is reset and all password history is lost.

Default The default history value is 0, which will disable the history functionality.

Mode Global Configuration

Examples To restrict reuse of the three most recent passwords, use the command:

```
awplus# configure terminal
awplus(config)# security-password history 3
```

To allow the reuse of recent passwords, use the command:

```
awplus# configure terminal
awplus(config)# no security-password history
```

Related commands

- [security-password forced-change](#)
- [security-password lifetime](#)
- [security-password min-lifetime-enforce](#)
- [security-password minimum-categories](#)
- [security-password minimum-length](#)
- [security-password reject-expired-pwd](#)
- [security-password warning](#)
- [show running-config security-password](#)
- [show security-password configuration](#)
- [show security-password user](#)

security-password forced-change

Overview This command specifies whether or not a user is forced to change an expired password at the next login. If this feature is enabled, users whose passwords have expired are forced to change to a password that must comply with the current password security rules at the next login.

Note that to use this command, the lifetime feature must be enabled with the [security-password lifetime](#) command and the reject-expired-pwd feature must be disabled with the [security-password reject-expired-pwd](#) command.

The **no** variant of the command disables this feature.

Syntax `security-password forced-change`
`no security-password forced-change`

Default The forced-change feature is disabled by default.

Mode Global Configuration

Example To force a user to change their expired password at the next login, use the command:

```
awplus# configure terminal
awplus(config)# security-password forced-change
```

Related commands

- [security-password history](#)
- [security-password lifetime](#)
- [security-password min-lifetime-enforce](#)
- [security-password minimum-categories](#)
- [security-password minimum-length](#)
- [security-password reject-expired-pwd](#)
- [security-password warning](#)
- [show running-config security-password](#)
- [show security-password configuration](#)
- [show security-password user](#)

security-password lifetime

Overview This command enables password expiry by specifying a password lifetime in days.

Note that when the password lifetime feature is disabled, it also disables the [security-password forced-change](#) command and the [security-password warning](#) command.

The **no** variant of the command disables this feature.

Syntax `security-password lifetime <0-1000>`
`no security-password lifetime`

Parameter	Description
<code><0-1000></code>	Password lifetime specified in days. A value of 0 will disable lifetime functionality and the password will never expire. This is equivalent to the no security-password lifetime command.

Default The default password lifetime is 0, which will disable the lifetime functionality.

Mode Global Configuration

Example To configure the password lifetime to 10 days, use the command:

```
awplus# configure terminal
awplus(config)# security-password lifetime 10
```

Related commands

- [security-password forced-change](#)
- [security-password history](#)
- [security-password min-lifetime-enforce](#)
- [security-password minimum-categories](#)
- [security-password minimum-length](#)
- [security-password reject-expired-pwd](#)
- [security-password warning](#)
- [show running-config security-password](#)
- [show security-password configuration](#)
- [show security-password user](#)

security-password min-lifetime-enforce

Overview Use this command to configure a minimum number of days before a password can be changed by a user. With this feature enabled, once a user sets the password, the user cannot change it again until the minimum lifetime has passed.

Use the **no** variant of this command to remove the minimum lifetime.

Syntax `security-password min-lifetime-enforce <0-1000>`
`no security-password min-lifetime-enforce`

Parameter	Description
<code><0-1000></code>	The minimum number of days before a password can be changed

Default By default, no minimum lifetime is enforced.

Mode Global Configuration

Usage notes The minimum lifetime is helpful in conjunction with a security policy that prevents people from re-using old passwords. For example, if you do not allow people to re-use any of their last 5 passwords, a person can bypass that restriction by changing their password 5 times in quick succession and then re-setting it to their previous password. The minimum lifetime prevents that by preventing people from changing their password in quick succession.

Example To force users to wait at least 2 days between changing passwords, use the command:

```
awplus(config)# security-password min-lifetime-enforce 2
```

Related commands

- [security-password forced-change](#)
- [security-password history](#)
- [security-password lifetime](#)
- [security-password minimum-categories](#)
- [security-password minimum-length](#)
- [security-password reject-expired-pwd](#)
- [security-password warning](#)
- [show running-config security-password](#)
- [show security-password configuration](#)
- [show security-password user](#)

Command changes Version 5.4.7-0.2: command added

security-password minimum-categories

Overview This command specifies the minimum number of categories that the password must contain in order to be considered valid. The password categories are:

- uppercase letters: A to Z
- lowercase letters: a to z
- digits: 0 to 9
- special symbols: all printable ASCII characters not included in the previous three categories. The question mark (?) cannot be used as it is reserved for help functionality.

Note that to ensure password security, the minimum number of categories should align with the lifetime selected, i.e. the fewer categories specified the shorter the lifetime specified.

Syntax `security-password minimum-categories <1-4>`

Parameter	Description
<1-4>	Number of categories the password must satisfy, in the range 1 to 4.

Default The default number of categories that the password must satisfy is 1.

Mode Global Configuration

Example To configure the required minimum number of character categories to be 3, use the command:

```
awplus# configure terminal
awplus(config)# security-password minimum-categories 3
```

Related commands

- [security-password forced-change](#)
- [security-password history](#)
- [security-password lifetime](#)
- [security-password min-lifetime-enforce](#)
- [security-password minimum-length](#)
- [security-password reject-expired-pwd](#)
- [security-password warning](#)
- [show running-config security-password](#)
- [show security-password configuration](#)
- [show security-password user](#)

security-password minimum-length

Overview This command specifies the minimum allowable password length. This value is checked against when there is a password change or a user account is created.

Syntax `security-password minimum-length <1-23>`

Parameter	Description
<code><1-23></code>	Minimum password length in the range from 1 to 23.

Default The default minimum password length is 1.

Mode Global Configuration

Example To configure the required minimum password length as 8, use the command:

```
awplus# configure terminal
awplus(config)# security-password minimum-length 8
```

Related commands

- [security-password forced-change](#)
- [security-password history](#)
- [security-password lifetime](#)
- [security-password min-lifetime-enforce](#)
- [security-password minimum-categories](#)
- [security-password reject-expired-pwd](#)
- [security-password warning](#)
- [show running-config security-password](#)
- [show security-password configuration](#)
- [show security-password user](#)

security-password reject-expired-pwd

Overview This command specifies whether or not a user is allowed to login with an expired password. Users with expired passwords are rejected at login if this functionality is enabled. Users then have to contact the Network Administrator to change their password.

CAUTION: *Once all users' passwords are expired you are unable to login to the device again if the security-password reject-expired-pwd command has been executed. You will have to reboot the device with a default configuration file, or load an earlier software version that does not have the security password feature.*

We recommend you never have the command line "security-password reject-expired-pwd" in a default config file.

Note that when the reject-expired-pwd functionality is disabled and a user logs on with an expired password, if the forced-change feature is enabled with [security-password forced-change](#) command, a user may have to change the password during login depending on the password lifetime specified by the [security-password lifetime](#) command.

The **no** variant of the command disables this feature.

Syntax `security-password reject-expired-pwd`
`no security-password reject-expired-pwd`

Default The reject-expired-pwd feature is disabled by default.

Mode Global Configuration

Example To configure the system to reject users with an expired password, use the command:

```
awplus# configure terminal
awplus(config)# security-password reject-expired-pwd
```

Related commands

- [security-password forced-change](#)
- [security-password history](#)
- [security-password lifetime](#)
- [security-password min-lifetime-enforce](#)
- [security-password minimum-categories](#)
- [security-password minimum-length](#)
- [security-password warning](#)
- [show running-config security-password](#)
- [show security-password configuration](#)
- [show security-password user](#)

security-password warning

Overview This command specifies the number of days before the password expires that the user will receive a warning message specifying the remaining lifetime of the password.

Note that the warning period cannot be set unless the lifetime feature is enabled with the [security-password lifetime](#) command.

The **no** variant of the command disables this feature.

Syntax `security-password warning <0-1000>`
`no security-password warning`

Parameter	Description
<0-1000>	Warning period in the range from 0 to 1000 days. A value 0 disables the warning functionality and no warning message is displayed for expiring passwords. This is equivalent to the no security-password warning command. The warning period must be less than, or equal to, the password lifetime set with the security-password lifetime command.

Default The default warning period is 0, which disables warning functionality.

Mode Global Configuration

Example To configure a warning period of three days, use the command:

```
awplus# configure terminal
awplus(config)# security-password warning 3
```

Related commands

- [security-password forced-change](#)
- [security-password history](#)
- [security-password lifetime](#)
- [security-password min-lifetime-enforce](#)
- [security-password minimum-categories](#)
- [security-password minimum-length](#)
- [security-password reject-expired-pwd](#)
- [show running-config security-password](#)
- [show security-password configuration](#)
- [show security-password user](#)

service advanced-vty

Overview This command enables the advanced-vty help feature. This allows you to use TAB completion for commands. Where multiple options are possible, the help feature displays the possible options.

The **no service advanced-vty** command disables the advanced-vty help feature.

Syntax `service advanced-vty`
`no service advanced-vty`

Default The advanced-vty help feature is enabled by default.

Mode Global Configuration

Examples To disable the advanced-vty help feature, use the command:

```
awplus# configure terminal
awplus(config)# no service advanced-vty
```

To re-enable the advanced-vty help feature after it has been disabled, use the following commands:

```
awplus# configure terminal
awplus(config)# service advanced-vty
```

service password-encryption

Overview Use this command to enable password encryption. This is enabled by default. When password encryption is enabled, the device displays passwords in the running config in encrypted form instead of in plain text.

Use the **no service password-encryption** command to stop the device from displaying newly-entered passwords in encrypted form. This does not change the display of existing passwords.

Syntax `service password-encryption`
`no service password-encryption`

Mode Global Configuration

Example `awplus# configure terminal`
`awplus(config)# service password-encryption`

Validation Commands `show running-config`

Related commands `enable password`

service telnet

Overview Use this command to enable the telnet server. The server is enabled by default. Enabling the telnet server starts the device listening for incoming telnet sessions on the configured port.

The server listens on port 23, unless you have changed the port by using the [privilege level](#) command.

Use the **no** variant of this command to disable the telnet server. Disabling the telnet server will stop the device listening for new incoming telnet sessions. However, existing telnet sessions will still be active.

Syntax `service telnet [ip|ipv6]`
`no service telnet [ip|ipv6]`

Default The IPv4 and IPv6 telnet servers are enabled by default.
The configured telnet port is TCP port 23 by default.

Mode Global Configuration

Examples To enable both the IPv4 and IPv6 telnet servers, use the following commands:

```
awplus# configure terminal
awplus(config)# service telnet
```

To enable the IPv6 telnet server only, use the following commands:

```
awplus# configure terminal
awplus(config)# service telnet ipv6
```

To disable both the IPv4 and IPv6 telnet servers, use the following commands:

```
awplus# configure terminal
awplus(config)# no service telnet
```

To disable the IPv6 telnet server only, use the following commands:

```
awplus# configure terminal
awplus(config)# no service telnet ipv6
```

Related commands [clear line vty](#)
[show telnet](#)
[telnet server](#)

show aaa local user locked

Overview This command displays the failed attempts against each user account attempting to login into the device, along with the failure times and locations.

Use this command's output to see if a user is currently locked out or not. You can check:

- the number of login attempts that have a 'V' in the 'Valid' column, and
- if the last attempt happened within the lockout time. If the number of 'V' attempts exceeds the maximum allowed number of attempts, and the last attempt is within the lockout time, then the user is locked out.

The maximum number of attempts is 5 by default. You can change it using the command **aaa local authentication attempts max-fail**. The lockout time is 5 minutes by default. You can change it using the command **aaa local authentication attempts lockout-time**.

Once a user's lockout status is cleared, this command will no longer display any failed attempts for that user. The status gets cleared by:

- being manually cleared by another privileged user, using the [clear aaa local user lockout](#) command, or
- the locked out user successfully logs into the system after waiting for the lockout time to pass.

In the Valid column:

- 'V' means this login attempt counts towards the maximum allowed number of attempts
- 'I' means this login attempt does not count towards the maximum allowed number of attempts, because it was more than 15 minutes ago.

Syntax `show aaa local user locked`

Mode User Exec and Privileged Exec

Example To display the current failed attempts for local users, use the command:

```
awplus# show aaa local user locked
```

Output Figure 4-1: Example output from the **show aaa local user locked** command

```
awplus#show aaa local user locked
manager:
When                Type  Source                Valid
2023-02-09 11:48:15 RHOST 192.168.5.1          V
2023-02-09 11:48:21 RHOST 192.168.5.1          V
user1:
When                Type  Source                Valid
2023-02-09 11:47:28 RHOST 192.168.5.1          V
2023-02-09 11:47:31 TTY   /dev/ttyS0           V
2023-02-09 11:47:35 TTY   /dev/ttyS0           V
2023-02-09 11:47:38 RHOST 192.168.5.1          V
2023-02-09 11:47:49 RHOST 192.168.5.1          V
2023-02-09 11:20:50 TTY   /dev/ttyS0           I
2023-02-09 11:20:54 RHOST 192.168.5.1          I
2023-02-09 11:47:19 RHOST 192.168.5.1          V
2023-02-09 11:47:23 TTY   /dev/ttyS0           V
user2:
When                Type  Source                Valid
2023-02-09 11:47:52 TTY   /dev/ttyS0           V
2023-02-09 11:47:55 RHOST 192.168.5.1          V
2023-02-09 11:47:58 TTY   /dev/ttyS0           V
2023-02-09 11:48:05 RHOST 192.168.5.1          V
2023-02-09 11:22:51 RHOST 192.168.5.1          I
2023-02-09 11:22:54 TTY   /dev/ttyS0           I
user3:
When                Type  Source                Valid
2023-02-09 11:38:58 TTY   /dev/ttyS0           V
2023-02-09 11:39:04 RHOST 192.168.5.1          V
2023-02-09 11:39:06 TTY   /dev/ttyS0           V
2023-02-09 11:39:22 RHOST 192.168.5.1          V
2023-02-09 11:39:26 TTY   /dev/ttyS0           V
```

This output example was run at 11:49. The lockout-time and max-fail settings are set to their defaults:

- manager: is not locked out because they only have 2 valid attempts.
- user1: is locked out because they have 7 valid attempts and the most recent was within the lockout time.
- user2: is not locked out because only 4 attempts are valid.
- user3: is not locked out. Even though they have 5 valid attempts, the most recent attempt is older than the lockout time of 5 minutes.

Related commands

- [aaa local authentication attempts lockout-time](#)
- [aaa local authentication attempts max-fail](#)
- [clear aaa local user lockout](#)

show privilege

Overview This command displays the current user privilege level, which can be any privilege level in the range <1-15>. Privilege levels <1-6> allow limited user access (all User Exec commands), privilege levels <7-14> allow restricted user access (all User Exec commands plus Privileged Exec show commands). Privilege level 15 gives full user access to all Privileged Exec commands.

Syntax `show privilege`

Mode User Exec and Privileged Exec

Usage notes A user can have an intermediate CLI security level set with this command for privilege levels <7-14> to access all show commands in Privileged Exec mode and all commands in User Exec mode, but no configuration commands in Privileged Exec mode.

Example To show the current privilege level of the user, use the command:

```
awplus# show privilege
```

Output Figure 4-2: Example output from the **show privilege** command

```
awplus#show privilege
Current privilege level is 15
awplus#disable
awplus>show privilege
Current privilege level is 1
```

Related commands [privilege level](#)

show security-password configuration

Overview This command displays the configuration settings for the various security password rules.

Syntax `show security-password configuration`

Mode Privileged Exec

Example To display the current security-password rule configuration settings, use the command:

```
awplus# show security-password configuration
```

Output Figure 4-3: Example output from the **show security-password configuration** command

```
Security Password Configuration
Minimum password length ..... 8
Minimum password character categories to match ..... 3
Number of previously used passwords to restrict..... 4
Password lifetime ..... 30 day(s)
  Warning period before password expires ..... 3 day(s)
Reject expired password at login ..... Disabled
  Force changing expired password at login ..... Enabled
```

Related commands

- [security-password forced-change](#)
- [security-password history](#)
- [security-password lifetime](#)
- [security-password min-lifetime-enforce](#)
- [security-password minimum-categories](#)
- [security-password minimum-length](#)
- [security-password reject-expired-pwd](#)
- [security-password warning](#)
- [show security-password user](#)

show security-password user

Overview This command displays user account and password information for all users.

Syntax `show security-password user`

Mode Privileged Exec

Example To display the system users' remaining lifetime or last password change, use the command:

```
awplus# show security-password user
```

Output Figure 4-4: Example output from the **show security-password** user command

User account and password information			
UserName	Privilege	Last-PWD-Change	Remaining-lifetime

manager	15	4625 day(s) ago	No Expiry
bob15	15	0 day(s) ago	30 days
ted7	7	0 day(s) ago	No Expiry
mike1	1	0 day(s) ago	No Expiry

Related commands

- [security-password forced-change](#)
- [security-password history](#)
- [security-password lifetime](#)
- [security-password min-lifetime-enforce](#)
- [security-password minimum-categories](#)
- [security-password minimum-length](#)
- [security-password reject-expired-pwd](#)
- [security-password warning](#)
- [show security-password configuration](#)

show telnet

Overview This command shows the Telnet server settings.

Syntax `show telnet`

Mode User Exec and Privileged Exec

Example To show the Telnet server settings, use the command:

```
awplus# show telnet
```

Output Figure 4-5: Example output from the **show telnet** command

```
Telnet Server Configuration
-----
Telnet server           : Enabled
Protocol                : IPv4, IPv6
Port                    : 23
```

Related commands

- [clear line vty](#)
- [service telnet](#)
- [show users](#)
- [telnet server](#)

show users

Overview This command shows information about the users who are currently logged into the device.

Syntax `show users`

Mode User Exec and Privileged Exec

Example To show the users currently connected to the device, use the command:

```
awplus# show users
```

Output Figure 4-6: Example output from the **show users** command

Line	User	Host(s)	Idle	Location	Priv	Idletime	Timeout
con 0	manager	idle	00:00:00	ttyS0	15	10	N/A
vtty 0	bob	idle	00:00:03	172.16.11.3	1	0	5

Table 1: Parameters in the output of the **show users** command

Parameter	Description
Line	Console port user is connected to.
User	Login name of user.
Host(s)	Status of the host the user is connected to.
Idle	How long the host has been idle.
Location	URL location of user.
Priv	The privilege level in the range 1 to 15, with 15 being the highest.
Idletime	The time interval the device waits for user input from either a console or VTY connection.
Timeout	The time interval before a server is considered unreachable.

strict-user-process-control

Overview Use this command to enable Strict User Process Control.

Strict User Process Control protects sensitive system resources from modification. It does this by preventing use of:

- some file and directory manipulation commands
- trigger scripting commands
- the **erase factory-default** command.

Use the **no** variant of this command to turn off Strict User Process Control.

Syntax `strict-user-process-control`
`no strict-user-process-control`

Default Disabled.

Mode Global Configuration

Usage notes When you enter the **strict-user-process-control** command, it prompts you for a password. Make the password different from any existing privileged management passwords. Store the password carefully and securely, because you will need it if you want to disable the feature.

In addition, the device will prompt you to save your configuration and reboot. This ensures the change takes effect correctly.

The command must be entered from a physical console; entering it from a remote login session is not allowed for extra security.

You can use the **show running-config** command to confirm whether Strict User Process Control is on or off. If the feature is running the output will contain the command **strict-user-process-control**.

Example To protect sensitive system files from access, use the commands:

```
awplus# configure terminal
awplus(config)# strict-user-process-control
```

Related commands [show running-config](#)
[strict-user-process-control force](#)

Command changes Version 5.5.2-2.1: command added

strict-user-process-control force

Overview Use this command to enable Strict User Process Control permanently, in a way that means it can never be disabled.

Strict User Process Control protects sensitive system resources from modification. It does this by preventing use of:

- some file and directory manipulation commands
- trigger scripting commands
- the **erase factory-default** command.

CAUTION: Only use this command if you have to do so for compliance with specific security certifications. Once you have turned this feature on, you will not be able to remove it.

Syntax `strict-user-process-control force`

Default Disabled.

Mode Global Configuration

Usage notes When you enter this command, the device will prompt you to save your configuration and reboot. This ensures the change takes effect correctly.

Unlike the **strict-user-process-control** command, this **strict-user-process-control force** command enables Strict User Process Control without prompting for or saving a password. This means you cannot disable Strict User Process Control using the **no** variant of the command (or in any other way).

The command must be entered from a physical console; entering it from a remote login session is not allowed for extra security.

You can use the **show running-config** command to confirm whether Strict User Process Control is on or off.

Example To permanently protect sensitive system files from access, use the commands:

```
awplus# configure terminal
awplus(config)# strict-user-process-control force
```

Related commands [show running-config](#)
[strict-user-process-control](#)

Command changes Version 5.5.4-1.8: command added

telnet

Overview Use this command to open a telnet session to a remote device.

Syntax `telnet {<hostname>| [ip] <ipv4-addr>| [ipv6] <ipv6-addr>}
[<port>]`

Parameter	Description
<hostname>	The host name of the remote system.
ip	Keyword used to specify the IPv4 address or host name of a remote system.
<ipv4-addr>	An IPv4 address of the remote system.
ipv6	Keyword used to specify the IPv6 address of a remote system
<ipv6-addr>	Placeholder for an IPv6 address in the format x:x::x:x, for example, 2001:db8::8a2e:7334
<port>	Specify a TCP port number (well known ports are in the range 1-1023, registered ports are 1024-49151, and private ports are 49152-65535).

Mode User Exec and Privileged Exec

Examples To connect to TCP port 2602 on the device at 10.2.2.2, use the command:

```
awplus# telnet 10.2.2.2 2602
```

To connect to the telnet server `host.example`, use the command:

```
awplus# telnet host.example
```

To connect to the telnet server `host.example` on TCP port 100, use the command:

```
awplus# telnet host.example 100
```

Command changes Version 5.4.6-2.1: VRF-lite support added.

telnet server

Overview This command enables the telnet server on the specified TCP port. If the server is already enabled then it will be restarted on the new port. Changing the port number does not affect the port used by existing sessions.

Syntax `telnet server {<1-65535>|default}`

Parameter	Description
<1-65535>	The TCP port to listen on.
default	Use the default TCP port number 23.

Mode Global Configuration

Example To enable the telnet server on TCP port 2323, use the following commands:

```
awplus# configure terminal
awplus(config)# telnet server 2323
```

Related commands [show telnet](#)

terminal length

Overview Use the **terminal length** command to specify the number of rows of output that the device will display before pausing, for the currently-active terminal only.

Use the **terminal no length** command to remove the length specified by this command. The default length will apply unless you have changed the length for some or all lines by using the [length \(asyn\)](#) command.

Syntax `terminal length <length>`
`terminal no length [<length>]`

Parameter	Description
<code><length></code>	<code><0-512></code> Number of rows that the device will display on the currently-active terminal before pausing.

Mode User Exec and Privileged Exec

Examples The following example sets the number of lines to 15:

```
awplus# terminal length 15
```

The following example removes terminal length set previously:

```
awplus# terminal no length
```

Related commands [terminal resize](#)
[length \(asyn\)](#)

terminal resize

Overview Use this command to automatically adjust the number of rows of output on the console, which the device will display before pausing, to the number of rows configured on the user's terminal.

Syntax `terminal resize`

Mode User Exec and Privileged Exec

Usage notes When the user's terminal size is changed, then a remote session via SSH or TELNET adjusts the terminal size automatically. However, this cannot normally be done automatically for a serial or console port. This command automatically adjusts the terminal size for a serial or console port.

Examples The following example automatically adjusts the number of rows shown on the console:

```
awplus# terminal resize
```

Related commands [length \(asyn\)](#)
[terminal length](#)

username

Overview This command creates or modifies a user to assign a privilege level and a password.

NOTE: The default username privilege level of 1 is not shown in running-config output. Any username privilege level that has been modified from the default is shown.

Syntax

```
username <name> privilege <1-15> [password [8] <password>]
username <name> password [8] <password>
no username <name>
```

Parameter	Description				
<name>	The login name for the user. Do not use punctuation marks such as single quotes ('), double quotes (" "), or colons (:) with the user login name.				
privilege	The user's privilege level. Use the privilege levels to set the access rights for each user. <table> <tr> <td><1-15></td><td> A privilege level: either 1-14 (limited access) or 15 (full access). A user with privilege level 1-14 can only access higher privilege levels if an enable password has been configured for the level the user tries to access and the user enters that password. A user at privilege level 1 can access the majority of show commands. A user at privilege level 7 can access the majority of show commands including platform show commands. Privilege Level 15 (to access the Privileged Exec command mode) is required to access configuration commands as well as show commands in Privileged Exec. </td></tr> </table>	<1-15>	A privilege level: either 1-14 (limited access) or 15 (full access). A user with privilege level 1-14 can only access higher privilege levels if an enable password has been configured for the level the user tries to access and the user enters that password. A user at privilege level 1 can access the majority of show commands. A user at privilege level 7 can access the majority of show commands including platform show commands. Privilege Level 15 (to access the Privileged Exec command mode) is required to access configuration commands as well as show commands in Privileged Exec.		
<1-15>	A privilege level: either 1-14 (limited access) or 15 (full access). A user with privilege level 1-14 can only access higher privilege levels if an enable password has been configured for the level the user tries to access and the user enters that password. A user at privilege level 1 can access the majority of show commands. A user at privilege level 7 can access the majority of show commands including platform show commands. Privilege Level 15 (to access the Privileged Exec command mode) is required to access configuration commands as well as show commands in Privileged Exec.				
password	A password that the user must enter when logging in. <table> <tr> <td>8</td><td> The parameter 8 means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form. Note that the user needs to enter the plain-text version of the password when logging in. </td></tr> <tr> <td><password></td><td> The user's password. The password can be up to 32 characters in length and include characters from up to four categories. The password categories are: - uppercase letters: A to Z - lowercase letters: a to z - digits: 0 to 9 - special symbols: all printable ASCII characters not included in the previous three categories. The question mark ? cannot be used as it is reserved for help functionality. </td></tr> </table>	8	The parameter 8 means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form. Note that the user needs to enter the plain-text version of the password when logging in.	<password>	The user's password. The password can be up to 32 characters in length and include characters from up to four categories. The password categories are: - uppercase letters: A to Z - lowercase letters: a to z - digits: 0 to 9 - special symbols: all printable ASCII characters not included in the previous three categories. The question mark ? cannot be used as it is reserved for help functionality.
8	The parameter 8 means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form. Note that the user needs to enter the plain-text version of the password when logging in.				
<password>	The user's password. The password can be up to 32 characters in length and include characters from up to four categories. The password categories are: - uppercase letters: A to Z - lowercase letters: a to z - digits: 0 to 9 - special symbols: all printable ASCII characters not included in the previous three categories. The question mark ? cannot be used as it is reserved for help functionality.				

Mode Global Configuration

Default The privilege level is 1 by default. Note the default is not shown in running-config output.

Usage notes An intermediate CLI security level (privilege level 7 to privilege level 14) allows a CLI user access to the majority of show commands, including the platform show commands that are available at privilege level 1 to privilege level 6. Note that some show commands, such as **show running-configuration** and **show startup-configuration**, are only available at privilege level 15.

Examples To create the user "bob" with a privilege level of 15, for all show commands including show running-configuration and show startup-configuration and to access configuration commands in Privileged Exec command mode, and the password "bobs_secret", use the commands:

```
awplus# configure terminal
```

```
awplus(config)# username bob privilege 15 password bobs_secret
```

To create a user "junior_admin" with a privilege level of 7, which will have intermediate CLI security level access for most show commands, and the password "show_only", use the commands:

```
awplus# configure terminal
```

```
awplus(config)# username junior_admin privilege 7 password  
show_only
```

Related commands

- [enable password](#)
- [security-password minimum-categories](#)
- [security-password minimum-length](#)

5

Subscription Licensing Commands

Introduction

Overview This chapter provides an alphabetical reference for each of the Subscription Licensing commands.

Subscription Licensing enables you to use the advanced threat protection features on your UTM firewall. To see the advanced threat protection subscriptions for your device, see the [Datasheet](#).

Subscription Licensing enables you to use Allied Telesis Management Framework (AMF). You need to purchase an AMF subscription for each AMF master or controller node in your AMF network. To see the AMF subscriptions for your device, see the [AlliedWare Plus Datasheet](#).

For step-by-step instructions about how to license AlliedWare Plus devices, see the [Licensing Feature Overview and Configuration Guide](#).

- Command List**
- “[license update file](#)” on page 209
 - “[license update online](#)” on page 210
 - “[show license external](#)” on page 211

license update file

Overview Use this command to load a license, after you have manually copied the license file onto the device.

Syntax `license update file <filename>`

Parameter	Description
<code><filename></code>	Name and path of the license file on the device.

Mode Privileged Exec

Examples To load a license onto a device from a file called "license_file.lic" that is stored at the top level of Flash memory, use the following command:

```
awplus# license update file license_file.lic
```

Related commands [show license external](#)

license update online

Overview From January 2025, this command is no longer available.

To install a subscription license, obtain the license file from your Allied Telesis representative, copy it onto the device, and use the command [license update file](#) to load the file.

For step-by-step instructions, see the [Licensing Feature Overview and Configuration Guide](#).

show license external

Overview Use this command to show information about subscription (external) licenses.

Syntax `show license external`

Mode Privileged Exec

Usage notes If you use AMF Recovery to replace a failed device with a new one, you have to transfer the license to the new switch within 28 days. The command output of **show license external** displays a message with instructions for doing this.

Examples To show information about what subscription features the device is licensed for, use the following command:

```
awplus#show license external
```

Output Figure 5-1: Example output from **show license external**

```
awplus#show license external
Licensed features:

Application Control (Procera)
Start date           : 24-Feb-2024 12:00AM
Expiry date          : 24-Feb-2025 11:59PM

Web Control (Digital Arts)
Start date           : 24-Feb-2024 12:00AM
Expiry date          : 24-Feb-2025 11:59PM
```

Related commands [license update file](#)

6

Update Manager Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to update a resource. For more information, see the [Update Manager Feature Overview and Configuration_Guide](#).

- Command List**
- “[show resource](#)” on page 213
 - “[update now](#)” on page 215

show resource

Overview Use this command to show information about resources used by enabled features running either locally or offloaded.

Syntax `show resource [<resource-name>]`

Parameter	Description
<code><resource-name></code>	Specific resource to show

Mode Privileged Exec

Examples To show information about the resources of features that have been enabled, use the following command:

```
awplus# show resource
```

Output Figure 6-1: Example output for **show resource**

```
awplus#show resource
```

Resource Name	Status	Version	Interval	Last Download	Next Download	Check
webgui	Sleeping	-	1 hour	None	Sun 1 Jul 2020 21:58:54	
dpi_procera_app_db	Sleeping	dpi_procera_app_db_v66	1 hour	None	Sun 1 Jul 2020 21:58:54	
afa_offload	Sleeping	afa_main_offload_v51	1 hour	None	Sun 1 Jul 2020 21:47:41	
iprep_et_rules	Sleeping	iprep_et_rules_v8582	1 hour	Mon 2 Jul 2020 04:05:06	Mon 2 Jul 2020 06:05:03	

The parameters in the example output are explained in the following table.

Parameter	Description
Resource Name	Name of the updatable resource
Status	Resource status. There are five types of status: Sleeping, Checking, Starting, Downloading, Stopping.
Version	Current version of the resource
Interval	Configured update check interval for the resource

Parameter	Description
Last Download	Time stamp of last resource downloaded
Next Download Check	Time stamp of next download check for the resource

Related commands

[update-interval \(antivirus\)](#)
[update-interval \(dpi\)](#)
[update-interval \(IP Reputation\)](#)
[update-interval \(malware\)](#)
[update now](#)

Command changes

Version 5.4.9-2.1: command added to SBx908 GEN2

update now

Overview Use this command to immediately perform a resource update check and update the specified resource if a newer version is available.

Syntax `update {<resource-name>|all} now`

Parameter	Description
<code><resource-name></code>	Specific resource to update. You will get an error message if the resource does not exist.
<code>all</code>	Update all resources

Mode Privileged Exec

Usage notes The default update interval for a resource is 1 hour. Users can initiate an immediate update check for a resource at any time without affecting any configured update check schedule. The Update Manager will perform an update check for a resource when triggered to do so. The Update Manager will request the current version number of the resource from the Update Server, then compare it with the current local version. If they are different, the Update Manager will initiate an update of the local resource.

Note that if a feature is disabled, regular and manual update checks for its resources are also disabled.

Also note that an update check for a resource will not proceed if an update of that resource is already in progress.

The Update Manager will retry upon failure to download a resource file because of DNS resolution error, bad checksum and so on.

Examples To do an update check and update all available resources, use the following command:

```
awplus# update all now
```

To do an update check and update the IP Reputation feature, use the following command:

```
awplus# update iprep_et_rules now
```

Related commands

[show resource](#)
[update-interval \(antivirus\)](#)
[update-interval \(dpi\)](#)
[update-interval \(IP Reputation\)](#)
[update-interval \(malware\)](#)

Command changes Version 5.4.9-2.1: command added to SBx908 GEN2

7

Web Redirect Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Web Redirect.

The Web Redirect feature monitors HTTP requests passing through a device, intercepts the request, and replies with an HTTP Redirect message instructing the client to go to a specified URL.

For more information, see the [Web Redirect Feature Overview and Configuration Guide](#).

- Command List**
- ["browser-only \(web-redirect\)"](#) on page 217
 - ["enable \(web-redirect\)"](#) on page 218
 - ["exclude app"](#) on page 219
 - ["exclude dst-ip"](#) on page 221
 - ["exclude ip"](#) on page 223
 - ["exclude mac"](#) on page 224
 - ["exclude url"](#) on page 225
 - ["idle-time \(web-redirect\)"](#) on page 227
 - ["mode \(web-redirect\)"](#) on page 229
 - ["proxy-host \(web-redirect\)"](#) on page 231
 - ["repeat-time \(web-redirect\)"](#) on page 233
 - ["server-url \(web-redirect\)"](#) on page 234
 - ["show running-config web-redirect"](#) on page 235
 - ["show web-redirect"](#) on page 236
 - ["web-redirect"](#) on page 237

browser-only (web-redirect)

Overview Use this command to redirect only the HTTP requests sent by a web browser.
Use the **no** variant of this command to redirect all HTTP requests.

Syntax browser-only
no browser-only

Default Disabled.

Mode Web Redirect Configuration

Usage notes Hosts may be using HTTP to request automatic software updates but it may be inappropriate for these requests to be redirected.

The **browser-only** option identifies browser requests by the "Mozilla" string in the User-Agent field of the HTTP request. If the string is not present the request is not redirected. All common browsers include "Mozilla" in their User-Agent field.

Example To redirect only web browser HTTP clients, use the following commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# browser-only
```

To redirect all HTTP clients, use the following commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# no browser-only
```

Related commands [web-redirect](#)

Command changes Version 5.4.8-1.1: command added

enable (web-redirect)

Overview Use this command to enable web redirection on a device.

Use the **no** variant of this command to disable web redirection without losing any existing web redirection configuration.

Syntax enable
no enable

Default Disabled.

Mode Web Redirect Configuration

Usage notes The web redirect feature monitors HTTP requests passing through a device, intercepts the request, and replies with an HTTP Redirect message instructing the client to go to a specified URL.

Example To enable web redirection, use the following commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# enable
```

To disable web redirection, use the following commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# no enable
```

Related commands [web-redirect](#)

Command changes Version 5.4.8-1.1: command added

exclude app

Overview Use this command to prevent web redirection from redirecting flows from a specified application.

Use the **no** variant of this command to remove an application-based exclusion.

Syntax `exclude app <application-name>`
`no exclude app <application-name>`

Parameter	Description
<code><application-name></code>	The application name.

Default Disabled

Mode Web Redirect Configuration

Usage notes In **proxy** mode, web redirection forwards all HTTP/HTTPS traffic to an upstream proxy server. You can use this command in proxy mode to exempt low security risk traffic from web redirection and send it directly to the Internet. This reduces the load on the proxy server.

Example To prevent the office365 application from having web-redirection applied, first set the **mode** to **proxy**:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# mode proxy
```

Then configure the **proxy-host** server address and port:

```
awplus(config-web-redirect)# proxy-host 192.168.1.1 port 80
```

Finally use the **exclude app** command:

```
awplus(config-web-redirect)# exclude app office365
```

To remove this exclusion, use the command:

```
awplus(config-web-redirect)# no exclude app office365
```

Related commands

- [browser-only \(web-redirect\)](#)
- [exclude dst-ip](#)
- [exclude ip](#)
- [exclude mac](#)
- [exclude url](#)
- [web-redirect](#)

Command changes Version 5.5.0-2.3: command added

exclude dst-ip

Overview Use this command to prevent web redirection from redirecting flows that have a specified destination IP address or network. You can use this to avoid redirecting requests for a particular server.

Use the **no** variant of this command to remove a destination IP address-based exclusion.

Syntax

```
exclude dst-ip  
{<ip-address>|<ip-subnet>|<ipv6-address>|<ipv6-prefix>}  
  
no exclude dst-ip  
{<ip-address>|<ip-subnet>|<ipv6-address>|<ipv6-prefix>}
```

Parameter	Description
<ip-address>	Exclude a specific server IP address from web redirection. Specify the address in dotted decimal format (A.B.C.D).
<ip-subnet>	Exclude a server subnet from web redirection. Specify the subnet in dotted decimal format (A.B.C.D/M).
<ipv6-address>	Exclude a specific server IPv6 address from web redirection. Specify the address in the format X:Y::Z.
<ipv6-prefix>	Exclude a server subnet from web redirection. Specify the prefix in the format X:Y::/Z.

Mode Web Redirect Configuration

Example To prevent requests to web servers in the subnet 192.168.5.0/24 from having web-redirection applied, use the commands:

```
awplus# configure terminal  
awplus(config)# web-redirect  
awplus(config-web-redirect)# exclude dst-ip 192.168.5.0/24
```

To remove this exclusion, use the commands:

```
awplus# configure terminal  
awplus(config)# web-redirect  
awplus(config-web-redirect)# no exclude dst-ip 192.168.5.0/24
```

Related commands

- [browser-only \(web-redirect\)](#)
- [exclude app](#)
- [exclude dst-ip](#)
- [exclude ip](#)
- [exclude mac](#)
- [exclude url](#)

web-redirect

Command changes Version 5.5.2-1.1: command added

exclude ip

Overview Use this command to prevent web redirection from redirecting flows that come from a specified source IP address or network.

Use the **no** variant of this command to remove a source IP address-based exclusion.

Syntax `exclude ip {<ip-address>|<ip-subnet>}`
`no exclude ip {<ip-address>|<ip-subnet>}`

Parameter	Description
<code><ip-address></code>	Exclude a specific client IP address from web redirection
<code><ip-subnet></code>	Exclude a client subnet from web redirection

Mode Web Redirect Configuration

Example To exclude the source subnet 192.0.2.0/24 from being redirected, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# exclude ip 192.0.2.0/24
```

To remove this exclusion, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# no exclude ip 192.0.2.0/24
```

Related commands [browser-only \(web-redirect\)](#)

[exclude app](#)
[exclude dst-ip](#)
[exclude ip](#)
[exclude mac](#)
[exclude url](#)
[web-redirect](#)

Command changes Version 5.4.8-1.1: command added

exclude mac

Overview Use this command to prevent web redirection from redirecting flows from a group of MAC addresses.

Use the **no** variant of this command to remove a MAC address-based exclusion.

Syntax `exclude mac <oui>`
`no exclude mac <oui>`

Parameter	Description
<oui>	The OUI (Organizational Unique Identifier) for the MAC address to be excluded. This is the vendor component of the MAC address, the first 24 bits that uniquely identify the vendor. It is in the format aa:bb:cc.

Mode Web Redirect Configuration

Usage notes Note that MAC address exclusions will not work for IPv6-based requests.

Example To prevent Allied Telesis devices from being redirected, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# exclude mac 00:00:cd
```

To remove this exclusion, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# no exclude mac 00:00:cd
```

Related commands [browser-only \(web-redirect\)](#)
[exclude app](#)
[exclude dst-ip](#)
[exclude ip](#)
[exclude url](#)
[web-redirect](#)

Command changes Version 5.4.8-1.1: command added

exclude url

Overview Use this command to prevent web redirection from redirecting flows that are going to a specified URL or group of URLs.

Use the **no** variant of this command to remove a URL-based exclusion.

Syntax `exclude url <regex>`
`no exclude url <regex>`

Parameter	Description
<code><regex></code>	A case sensitive regular expression used to check a URL for a match. If the URL matches the regular expression it is excluded from web redirection.

Default Disabled

Mode Web Redirect Configuration

Usage notes In **proxy** mode, web redirection forwards all HTTP/HTTPS traffic to an upstream proxy server. You can use this command in proxy mode to exempt low security risk traffic from web redirection and send it directly to the Internet. This reduces the load on the proxy server.

Example To prevent all URLs containing 'example.com' from having web-redirection applied, first set the **mode** to proxy:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# mode proxy
```

Then configure the **proxy-host** server address and port:

```
awplus(config-web-redirect)# proxy-host 192.168.1.1 port 80
```

Finally use the **exclude url** command:

```
awplus(config-web-redirect)# exclude url example.com
```

To remove the exclusion for all URLs ending with 'example.com', use the command:

```
awplus(config-web-redirect)# no exclude url example.com
```

Other examples To exclude all URLs that contain the word 'mail', use the following regular expression:

```
awplus(config-web-redirect)# exclude url mail
```

To exclude all URLs that start with 'https://', use the following regular expression:

```
awplus(config-web-redirect)# exclude url ^https://
```

To exclude a specific URL, use the following regular expression:

```
awplus(config-web-redirect)# exclude url  
^https://www.example.com/Doc/FAQ/$
```

**Related
commands**

[browser-only \(web-redirect\)](#)

[exclude app](#)

[exclude dst-ip](#)

[exclude ip](#)

[exclude mac](#)

[web-redirect](#)

**Command
changes**

Version 5.5.0-2.3: command added

idle-time (web-redirect)

Overview Use this command to set the time the client must have been idle before it can be redirected once the repeat-time has expired.

This command improves your web browsing experience. For example, if you were busy browsing a web site and loading new content, then it is undesirable to be immediately redirected after the expiry of the repeat time interval. To ensure an ideal user experience, it is better to wait for an additional period of time to ensure current web site content is fully downloaded, and for the browser to have been idle before being redirected.

Use the **no** variant of this command to revert to the default value of 0.

Syntax `idle-time <0-86400>`
`no idle-time`

Parameter	Description
<code><0-86400></code>	Idle time after repeat time before redirecting a client, in seconds.

Default 0 seconds.

Mode Web Redirect Configuration

Usage notes Sets the interval, following the repeat time, for which a client must be idle before it will be redirected again. This interval makes it likely that it will be a web page request that is redirected, rather than some sub-component of the page. This ensures the page that the user is being redirected to is displayed as a full page, rather than a sub-component of the current page being browsed to.

NOTE: *The time when the client is idle can include the time leading up to the expiry of the **repeat-time**. So, if the idle time was 60sec and the client had been idle for the 60sec prior to the repeat-time expiring, the client could be redirected straight away. Or, if it had been idle for 30sec prior to the repeat-time expiring, it would need to be idle for a further 30sec afterwards, before being redirected.*

Example To configure the time after repeat time before redirecting a client to 1 hour (3600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# idle-time 3600
```

To restore the default idle time, which is 0 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# no idle-time
```

Related commands	web-redirect
	repeat-time (web-redirect)
Command changes	Version 5.4.8-1.1: command added

mode (web-redirect)

Overview Use this command to set the Web Redirection mode.

Use the **no** variant of this command to revert to the default mode of HTTP redirection.

Syntax mode {http|proxy}
no mode

Parameter	Description
http	HTTP and HTTPS redirection. This provides a way for HTTP and HTTPS client requests to be redirected to a specified URL.
proxy	Proxy chaining redirection. In proxy chaining mode, Web Redirect forwards all HTTP/HTTPS traffic to a particular upstream explicit proxy server.

Default HTTP.

Mode Web Redirect Configuration

Example To set the web redirection to proxy chaining mode, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# mode proxy
```

To set the web redirection to HTTP mode, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# mode http
```

To restore the default web redirection, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# no mode
```

Related commands

[web-redirect](#)
[repeat-time \(web-redirect\)](#)
[idle-time \(web-redirect\)](#)
[server-url \(web-redirect\)](#)
[browser-only \(web-redirect\)](#)
[show running-config web-redirect](#)

exclude ip
exclude mac
exclude app
show web-redirect

Command changes Version 5.5.0-2.3: command added

proxy-host (web-redirect)

Overview Use this command to configure the proxy server host and port for Web Redirect in proxy chaining mode.

In proxy chaining mode, Web Redirect forwards all HTTP/HTTPS traffic to the specified upstream proxy server.

Use the **no** variant of this command to remove a configured proxy server host and port.

Syntax `proxy-host {<ipv4-address>|<ipv6-address>|<host-name>} port <0-65535>`
`no proxy-host`

Parameter	Description
<ipv4-address>	IPv4 address in dotted decimal format, for example, 192.0.2.2.
<ipv6-address>	IPv6 address in the format x:x::x:x for example, 2001:db8::8a2e:7334.
<host-name>	The host name. You can use all alphanumeric ASCII characters, and the dash (-) and underscore (_) characters. The name can be 1 to 64 characters in long.
port	The port number in the range of 0-65535.

Default Disabled.

Mode Web Redirect Configuration

Example To configure a proxy server host of IP address 10.1.1.1 and port number 1234, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# proxy-host 10.1.1.1 port 1234
```

To remove the configuration, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# no proxy-host
```

Related commands [web-redirect](#)
[repeat-time \(web-redirect\)](#)
[idle-time \(web-redirect\)](#)
[server-url \(web-redirect\)](#)

browser-only (web-redirect)
show running-config web-redirect
exclude ip
exclude mac
exclude app
show web-redirect
mode (web-redirect)
exclude url

Command changes Version 5.5.0-2.3: command added

repeat-time (web-redirect)

Overview Use this command to configure the interval time between redirects for a client. Use the **no** variant of this command to revert to the default interval time.

Syntax `repeat-time <1-31536000>`
`no repeat-time`

Parameter	Description
<code><1-31536000></code>	The interval between redirects for a client in seconds.

Default 0 seconds.

Mode Web Redirect Configuration

Usage notes Sets the interval (in seconds) between redirects for a client. After the specified interval the client will be eligible to be redirected again. If no **repeat-time** is specified every client request will be eligible for a redirect immediately. Whether or not an eligible client is immediately redirected at the expiry of the repeat time depends on the idle-time.

Example To set the interval time between redirects to every hour (3600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# repeat-time 3600
```

To restore the default repeat time interval time between re-directs (0 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# no repeat-time
```

Related commands [idle-time \(web-redirect\)](#)
[web-redirect](#)

Command changes Version 5.4.8-1.1: command added

server-url (web-redirect)

Overview Use this command to configure the URL of the server to which the HTTP connection will be redirected.

Use the **no** variant of this command to remove the configured server redirect URL.

Syntax `server-url <url>`
`no server-url`

Parameter	Description
<code><url></code>	URL (host name or dotted IP notation)

Mode Web Redirect Configuration

Example To redirect the HTTP connection to `http://redirectexample.com`, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# server-url
http://redirectexample.com
```

To unset the server redirect URL, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)# no server-url
```

Related commands [web-redirect](#)

Command changes Version 5.4.8-1.1: command added

show running-config web-redirect

Overview Use this command to display the running configuration for web redirection.

Syntax `show running-config web-redirect`

Mode Privileged Exec

Example To display the running configuration for web redirection, use the following commands:

```
awplus# show running-config web-redirect
```

Output Figure 7-1: Example output from **show running-config web-redirect**

```
awplus#show running-config web-redirect
web-redirect
server-url http://redirectexample.com
repeat-time 3600
idle-time 360
enable!
```

Related commands [web-redirect](#)

Command changes Version 5.4.8-1.1: command added.

show web-redirect

Overview Use this command to display information about the status of web redirect, the total number of redirected hosts being tracked, and information about when each host (by IP) was last redirected and when it will next be eligible for redirection.

Syntax `show web-redirect`

Mode Privileged Exec

Example To show the state of web redirection, use the following command:

```
awplus# show web-redirect
```

Output Figure 7-2: Example output from **show web-redirect**

```
awplus#show web-redirect
Mode:      HTTP redirection
Status:     Enabled
Total number of redirected clients: 5
Clients:
Address                Last Redirection                Next redirection after
-----
192.0.2.0.2            Tue 22 Jun 2021 11:03:50        Wed 23 Jun 2021 11:03:50
192.0.2.0.17           Tue 22 Jun 2021 10:51:11        Wed 23 Jun 2021 10:51:11
192.0.2.0.31           Tue 22 Jun 2021 05:33:42        Wed 23 Jun 2021 05:33:42
2001:db8::2:121        Tue 22 Jun 2021 17:48:06        Wed 23 Jun 2021 17:48:06
2001:db8::1:ab6d       Tue 22 Jun 2021 01:18:39        Wed 23 Jun 2021 01:18:39
```

Related commands [web-redirect](#)

Command changes Version 5.4.8-1.1: command added

web-redirect

Overview Use this command to enter the web redirection mode so you can configure web redirection.

Use the **no** variant of this command to remove all web redirection configuration.

Syntax `web-redirect`
`no web-redirect`

Default Disabled

Mode Global Configuration

Example To configure the web redirection settings, use the commands:

```
awplus# configure terminal
awplus(config)# web-redirect
awplus(config-web-redirect)#
```

To remove all web redirection configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no web-redirect
```

Related commands

- [enable \(web-redirect\)](#)
- [server-url \(web-redirect\)](#)
- [browser-only \(web-redirect\)](#)
- [exclude app](#)
- [exclude dst-ip](#)
- [exclude ip](#)
- [exclude mac](#)
- [exclude url](#)
- [show running-config web-redirect](#)
- [show web-redirect](#)

Command changes Version 5.4.8-1.1: command added

8

System Configuration and Monitoring Commands

Introduction

Overview This chapter provides an alphabetical reference of commands for configuring and monitoring the system.

- Command List**
- ["banner display external-manager"](#) on page 240
 - ["banner exec"](#) on page 241
 - ["banner external-manager"](#) on page 243
 - ["banner login \(system\)"](#) on page 245
 - ["banner motd"](#) on page 247
 - ["clock summer-time date"](#) on page 249
 - ["clock summer-time recurring"](#) on page 251
 - ["clock timezone"](#) on page 253
 - ["debug core-file"](#) on page 254
 - ["hostname"](#) on page 255
 - ["low-memory restart"](#) on page 257
 - ["max-fib-routes"](#) on page 258
 - ["max-static-routes"](#) on page 259
 - ["no debug all"](#) on page 260
 - ["reboot"](#) on page 262
 - ["reload"](#) on page 263
 - ["show banner external-manager"](#) on page 264
 - ["show clock"](#) on page 265
 - ["show cpu"](#) on page 267
 - ["show cpu history"](#) on page 270

- [“show debugging”](#) on page 272
- [“show memory”](#) on page 273
- [“show memory allocations”](#) on page 275
- [“show memory history”](#) on page 277
- [“show memory pools”](#) on page 278
- [“show memory shared”](#) on page 279
- [“show process”](#) on page 280
- [“show reboot history”](#) on page 282
- [“show router-id”](#) on page 283
- [“show system”](#) on page 284
- [“show system mac”](#) on page 285
- [“show system serialnumber”](#) on page 286
- [“show tech-support”](#) on page 287
- [“terminal monitor”](#) on page 289
- [“undebg all”](#) on page 290

banner display external-manager

Overview Use this command to display the external-manager banner. The external-manager banner warns you that certain features are being managed by an external management system. For example, if you are using Vista Manager EX to manage your network, you will see a notification banner telling you what features are being managed after you enter Global Configuration Mode.

Use the **no** variant of this command to hide the external-manager banner.

Syntax `banner display external-manager`
`no banner display external-manager`

Default The external-manager banner is displayed by default.

Mode User Exec

Usage notes The external-manager banner is displayed by default. In some instances it is desirable to hide it for the current session. You do this by using the **no** variant of this command. The banner will remain hidden until you either re-enable it, or log out and then log back in.

Example To hide the external-manager banner, use the command:

```
awplus> no banner display external-manager
```

To display the external-manager banner, use the command:

```
awplus> banner display external-manager
```

Related commands [banner external-manager](#)
[show banner external-manager](#)

Command changes Version 5.5.1-1.1: command added

banner exec

Overview This command configures the User Exec mode banner that is displayed on the console after you login. The **banner exec default** command restores the User Exec banner to the default banner. Use the **no banner exec** command to disable the User Exec banner and remove the default User Exec banner.

Syntax `banner exec <banner-text>`
`banner exec default`
`no banner exec`

Default By default, the AlliedWare Plus™ version and build date is displayed at console login, such as:

```
AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00
```

Mode Global Configuration

Examples To configure a User Exec mode banner after login (in this example, to tell people to use the **enable** command to move to Privileged Exec mode), enter the following commands:

```
awplus#configure terminal
awplus(config)#banner exec Use enable to move to Priv Exec mode
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

Use enable to move to Priv Exec mode

awplus>
```

To restore the default User Exec mode banner after login, enter the following commands:

```
awplus#configure terminal
awplus(config)#banner exec default
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00

awplus>
```

To remove the User Exec mode banner after login, enter the following commands:

```
awplus#configure terminal
awplus(config)#no banner exec
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

awplus>
```

Related commands [banner login \(system\)](#)
[banner motd](#)

banner external-manager

Overview Use this command to add an entry to the external-manager banner. The external-manager banner warns you that certain features are being managed by an external management system. For example, if you are using Vista Manager EX to manage your network, you will see a notification banner telling you what features are being managed after you enter Global Configuration Mode.

Use the **no** variant to remove an entry from the external-manager banner.

Syntax `banner external-manager <manager-name> feature <feature-name>
note <feature-note>`
`no banner external-manager <manager-name> [feature
<feature-name> note <feature-note>]`

Parameter	Description
<code><manager-name></code>	A string that describes the management system.
<code><feature-name></code>	A string that describes the feature being managed.
<code><feature-note></code>	A note for the feature.

Default No external-manager banner entries are configured by default.

Mode Global Configuration

Usage notes When you run this command:

- if no entry exists for an external manager, the external manager, feature and note are added.
- if an entry already exists for an external manager, the feature and note are added to the existing manager.
- if the feature already exists for that manager, then the note is added to the existing feature.

The **no** variant of this command removes the specified note from the feature of the specified external manager.

- If there are no other notes for the feature, then the feature is removed.
- If the feature is removed and there are no other features for the external manager, then the external manager is removed.

Use the **no** variant with just the external manager name to remove an external manager and all its features and notes.

Example To add an external manager note for 'Vista Manager' for the feature 'traffic-control' with the note 'Dynamic Traffic Management', use the commands:

```
awplus# configure terminal
awplus(config)# banner external-manager "Vista Manager" feature
"traffic-control" note "Dynamic Traffic Management"
```

To remove the external manager note 'Dynamic Traffic Management' from the feature 'traffic-control' of the external manager 'Vista Manager', use the commands:

```
awplus# configure terminal
awplus(config)# no banner external-manager "Vista Manager"
feature "traffic-control" note "Dynamic Traffic Management"
```

To remove all external manager features and notes for 'Vista Manager', use the commands:

```
awplus# configure terminal
awplus(config)# no banner external-manager "Vista Manager"
```

Related commands [banner display external-manager](#)
[show banner external-manager](#)

Command changes Version 5.5.1-1.1: command added

banner login (system)

Overview This command configures the login banner that is displayed on the console when you login. The login banner is displayed on all connected terminals. The login banner is displayed after the MOTD (Message-of-the-Day) banner and before the login username and password prompts.

Use the **no banner login** command to disable the login banner.

Syntax banner login
no banner login

Default By default, no login banner is displayed at console login.

Mode Global Configuration

Examples To configure a login banner of "Authorised users only" to be displayed when you login, enter the following commands:

```
awplus#configure terminal
awplus(config)#banner login
Type CNTL/D to finish.

Authorised users only

awplus(config)#exit
awplus#exit

Authorised users only

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00

awplus>
```

To remove the login banner, enter the following commands:

```
awplus#configure terminal
awplus(config)#no banner login
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00

awplus>
```

**Related
commands** [banner exec](#)
 [banner motd](#)

banner motd

Overview Use this command to create or edit the text MotD (Message-of-the-Day) banner displayed before login. The MotD banner is displayed on all connected terminals. The MotD banner is useful for sending messages that affect all network users, for example, any imminent system shutdowns.

Use the **no** variant of this command to delete the MotD banner.

Syntax `banner motd <motd-text>`
`no banner motd`

Parameter	Description
<code><motd-text></code>	The text to appear in the Message of the Day banner.

Default By default, the device displays the AlliedWare Plus™ OS version and build date when you login.

Mode Global Configuration

Examples To configure a MotD banner of "System shutdown at 6pm today" to be displayed when you log in, enter the following commands:

```
awplus>enable
awplus#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
awplus(config)#banner motd System shutdown at 6pm today
awplus(config)#exit
awplus#exit

System shutdown at 6pm today
awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00

awplus>
```

To delete the login banner, enter the following commands:

```
awplus>enable
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#no banner motd
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00

awplus>
```

**Related
commands**

[banner exec](#)

[banner login \(system\)](#)

clock summer-time date

Overview This command defines the start and end of summertime for a specific year only, and specifies summertime's offset value to Standard Time for that year.

The **no** variant of this command removes the device's summertime setting. This clears both specific summertime dates and recurring dates (set with the [clock summer-time recurring](#) command).

By default, the device has no summertime definitions set.

Syntax

```
clock summer-time <timezone-name> date <start-day>
<start-month> <start-year> <start-time> <end-day> <end-month>
<end-year> <end-time> <1-180>

no clock summer-time
```

Parameter	Description
<timezone-name>	A description of the summertime zone, up to 6 characters long.
date	Specifies that this is a date-based summertime setting for just the specified year.
<start-day>	Day that the summertime starts, from 1 to 31.
<start-month>	First three letters of the name of the month that the summertime starts.
<start-year>	Year that summertime starts, from 2000 to 2035.
<start-time>	Time of the day that summertime starts, in the 24-hour time format HH:MM.
<end-day>	Day that summertime ends, from 1 to 31.
<end-month>	First three letters of the name of the month that the summertime ends.
<end-year>	Year that summertime ends, from 2000 to 2035.
<end-time>	Time of the day that summertime ends, in the 24-hour time format HH:MM.
<1-180>	The offset in minutes.

Mode Global Configuration

Examples To set a summertime definition for New Zealand using NZST (UTC+12:00) as the standard time, and NZDT (UTC+13:00) as summertime, with the summertime set to begin on the 25th of September 2016 and end on the 2nd of April 2017:

```
awplus(config)# clock summer-time NZDT date 25 sep 2:00 2016 2
apr 2:00 2017 60
```

To remove any summertime settings on the system, use the command:

```
awplus(config)# no clock summer-time
```

**Related
commands** [clock summer-time recurring](#)
[clock timezone](#)

clock summer-time recurring

Overview This command defines the start and end of summertime for every year, and specifies summertime's offset value to Standard Time.

The **no** variant of this command removes the device's summertime setting. This clears both specific summertime dates (set with the [clock summer-time date](#) command) and recurring dates.

By default, the device has no summertime definitions set.

Syntax `clock summer-time <timezone-name> recurring <start-week>
<start-day> <start-month> <start-time> <end-week> <end-day>
<end-month> <end-time> <1-180>`
`no clock summer-time`

Parameter	Description
<timezone-name>	A description of the summertime zone, up to 6 characters long.
recurring	Specifies that this summertime setting applies every year from now on.
<start-week>	Week of the month when summertime starts, in the range 1-5. The value 5 indicates the last week that has the specified day in it for the specified month. For example, to start summertime on the last Sunday of the month, enter 5 for <start-week> and sun for <start-day>.
<start-day>	Day of the week when summertime starts. Valid values are mon, tue, wed, thu, fri, sat or sun.
<start-month>	First three letters of the name of the month that summertime starts.
<start-time>	Time of the day that summertime starts, in the 24-hour time format HH:MM.
<end-week>	Week of the month when summertime ends, in the range 1-5. The value 5 indicates the last week that has the specified day in it for the specified month. For example, to end summertime on the last Sunday of the month, enter 5 for <end-week> and sun for <end-day>.
<end-day>	Day of the week when summertime ends. Valid values are mon, tue, wed, thu, fri, sat or sun.
<end-month>	First three letters of the name of the month that summertime ends.
<end-time>	Time of the day that summertime ends, in the 24-hour time format HH:MM.
<1-180>	The offset in minutes.

Mode Global Configuration

Examples To set a summertime definition for New Zealand using NZST (UTC+12:00) as the standard time, and NZDT (UTC+13:00) as summertime, with summertime set to start on the last Sunday in September, and end on the 1st Sunday in April, use the command:

```
awplus(config)# clock summer-time NZDT recurring 5 sun sep 2:00  
1 sun apr 2:00 60
```

To remove any summertime settings on the system, use the command:

```
awplus(config)# no clock summer-time
```

Related commands [clock summer-time date](#)
[clock timezone](#)

clock timezone

Overview This command defines the device's clock timezone. The timezone is set as a offset to the UTC.

The **no** variant of this command resets the system time to UTC.

By default, the system time is set to UTC.

Syntax `clock timezone <timezone-name> {minus|plus}
[<0-13>|<0-12>:<00-59>]`
`no clock timezone`

Parameter	Description
<timezone-name>	A description of the timezone, up to 6 characters long.
minusorplus	The direction of offset from UTC. The minus option indicates that the timezone is behind UTC. The plus option indicates that the timezone is ahead of UTC.
<0-13>	The offset in hours or from UTC.
<0-12>:<00-59>	The offset in hours or from UTC.

Mode Global Configuration

Usage notes Configure the timezone before setting the local time. Otherwise, when you change the timezone, the device applies the new offset to the local time.

Examples To set the timezone to New Zealand Standard Time with an offset from UTC of +12 hours, use the command:

```
awplus(config)# clock timezone NZST plus 12
```

To set the timezone to Indian Standard Time with an offset from UTC of +5:30 hours, use the command:

```
awplus(config)# clock timezone IST plus 5:30
```

To set the timezone back to UTC with no offsets, use the command:

```
awplus(config)# no clock timezone
```

Related commands [clock summer-time date](#)
[clock summer-time recurring](#)

debug core-file

Overview Use this command to enable the generation of crash core files.
Use the **no** variant of this command to disable the generation of crash core files.

Syntax debug core-file
no debug core-file

Default Enabled.

Mode Global Configuration

Usage notes Core files may contain raw memory content. This may not be acceptable in a security certified network. Use the **no debug core-file** command to prevent such core files from being generated.

Example To prevent the generation of core files, use the commands:

```
awplus# configure terminal
awplus(config)# no debug core-file
```

Related commands [show system](#)

Command changes Version 5.4.9-1.0: command added

hostname

Overview This command sets the name applied to the device as shown at the prompt. The hostname is:

- displayed in the output of the [show system](#) command
- displayed in the CLI prompt so you know which device you are configuring
- stored in the MIB object sysName

Use the **no** variant of this command to revert the hostname setting to its default. For devices that are not part of an AMF network, the default is “awplus”.

Syntax `hostname <hostname>`
`no hostname [<hostname>]`

Parameter	Description
<code><hostname></code>	Specifies the name given to a specific device.

Default awplus

Mode Global Configuration

Usage notes Within an AMF network, any device without a user-defined hostname will automatically be assigned a name based on its MAC address.

To efficiently manage your network using AMF, we strongly advise that you devise a naming convention for your network devices and apply an appropriate hostname to each device.

The name must also follow the rules for ARPANET host names. The name must start with a letter, end with a letter or digit, and use only letters, digits, and hyphens. Refer to RFC 1035.

Example To set the system name to HQ-Sales, use the command:

```
awplus# configure terminal
awplus(config)# hostname HQ-Sales
```

This changes the prompt to:

```
HQ-Sales(config)#
```

To revert to the default hostname awplus, use the command:

```
HQ-Sales(config)# no hostname
```

This changes the prompt to:

```
awplus(config)#
```

NOTE: When AMF is configured, running the **no hostname** command will apply a hostname that is based on the MAC address of the device node, for example, **node_0000_5e00_5301**.

**Related
commands** [show system](#)

low-memory restart

Overview Use this command to specify a process for the device to terminate if available memory is sufficiently low.

This command is intended for use in consultation with Allied Telesis customer support. Using this command will make the device produce a core dump when the process terminates, which makes it easier for Allied Telesis engineers to debug any issues.

Use the **no** variant of this command to stop specifying the process for termination.

Syntax `low-memory restart <process-name>`
`no low-memory restart <process-name>`

Parameter	Description
<code><process-name></code>	The name of a process to terminate if the device memory gets sufficiently low.

Default None. By default, the device will automatically terminate the non-critical process that has the highest memory consumption. Note that only a non-critical process will be terminated automatically, not a critical process.

Mode Global Configuration

Usage notes The process does not have to be running when you enter this command. If it is running at the time the available memory becomes sufficiently low, the device will terminate it.

Example To specify RIP as the process to terminate if memory gets too low, use the commands:

```
awplus# configure terminal
awplus(config)# low-memory restart ripd
```

Related commands [show memory](#)
[snmp-server enable trap](#)

Command changes Version 5.5.4-2.3: command added

max-fib-routes

Overview This command enables you to control the maximum number of FIB routes configured. It operates by providing parameters that enable you to configure preset maximums and warning message thresholds.

NOTE: For static routes use the [max-static-routes](#) command.

Use the **no** variant of this command to set the maximum number of FIB routes to the default of 4294967294 FIB routes.

Syntax `max-fib-routes <1-4294967294> [<1-100>|warning-only]`
`no max-fib-routes`

Parameter	Description
max-fib-routes	This is the maximum number of routes that can be stored in the device's Forwarding Information dataBase. In practice, other practical system limits would prevent this maximum being reached.
<1-4294967294>	The allowable configurable range for setting the maximum number of FIB-routes.
<1-100>	This parameter enables you to optionally apply a percentage value. This percentage will be based on the maximum number of FIB routes you have specified. This will cause a warning message to appear when your routes reach your specified percentage value. Routes can continue to be added until your configured maximum value is reached.
warning-only	This parameter enables you to optionally apply a warning message. If you set this option a warning message will appear if your maximum configured value is reached. Routes can continue to be added until your device reaches either the maximum capacity value of 4294967294, or a practical system limit.

Default The default number of FIB routes is the maximum number of FIB routes (4294967294).

Mode Global Configuration

Examples To set the maximum number of dynamic routes to 2000 and warning threshold of 75%, use the following commands:

```
awplus# config terminal
awplus(config)# max-fib-routes 2000 75
```

max-static-routes

Overview Use this command to set the maximum number of static routes, excluding FIB (Forwarding Information Base) routes.

NOTE: For FIB routes use the [max-fib-routes](#) command.

Use the **no** variant of this command to set the maximum number of static routes to the default of 1024 static routes.

Syntax max-static-routes <1-1024>
no max-static-routes

Default The default number of static routes is the maximum number of static routes (1024).

Mode Global Configuration

Example To reset the maximum number of static routes to the default maximum, use the command:

```
awplus# configure terminal
awplus(config)# no max-static-routes
```

NOTE: Static routes are applied before adding routes to the RIB (Routing Information Base). Therefore, rejected static routes will not appear in the running config.

Related commands [max-fib-routes](#)

no debug all

Overview This command disables the debugging facility for all features on your device. This stops the device from generating any diagnostic debugging messages.

You can optionally disable the debugging facility for only the given protocol or feature. The features available depend on your device and will be a subset of the features listed in the Syntax section below.

Syntax `no debug all [bgp|ipv6 ospf|ipv6 rip|dot1x|nsm|ospf|pim
dense-mode|pim sparse-mode|rip|vrrp]`

Parameter	Description
bgp	Turns off all debugging for BGP (Border Gateway Protocol).
dot1x	Turns off all debugging for IEEE 802.1X port-based network access- control.
ipv6 ospf	Turns off all debugging for IPv6 OSPF (Open Shortest Path First).
ipv6 rip	Turns off all debugging for IPv6 RIP (Routing Information Protocol).
nsm	Turns off all debugging for the NSM (Network Services Module).
ospf	Turns off all debugging for OSPF (Open Shortest Path First).
pim dense-mode	Turns off all debugging for PIM (Protocol Independent Multicast) Dense Mode.
pim sparse-mode	Turns off all debugging for PIM (Protocol Independent Multicast) Sparse Mode.
rip	Turns off all debugging for RIP (Routing Information Protocol).
vrrp	Turns off all debugging for VRRP (Virtual Router Redundancy Protocol).

Default Disabled

Mode Global Configuration and Privileged Exec

Example To disable debugging for all features, use the command:

```
awplus# no debug all
```

To disable all BGP debugging, use the command:

```
awplus# no debug all bgp
```

To disable all NSM debugging, use the command:

```
awplus# no debug all nsm
```


To disable all OSPF debugging, use the command:

```
awplus# no debug all ospf
```

To disable all PIM Sparse Mode debugging, use the command:

```
awplus# no debug all pim sparse-mode
```

To disable all RIP debugging, use the command:

```
awplus# no debug all rip
```

To disable all VRRP debugging, use the command:

```
awplus# no debug all vrrp
```

**Related
commands** [undebug all](#)

**Command
changes** Version 5.4.7-1.1: **pim dense-mode**, **pim sparse-mode**, and **rip** parameters added

reboot

Overview This command halts the device and performs a cold restart (also known as reload). It displays a confirmation request before restarting.

Syntax `reboot`
`reload`

Mode Privileged Exec

Usage notes The **reboot** and **reload** commands perform the same action.

Examples To restart the device, use the command:

```
awplus# reboot
reboot system? (y/n): y
```

reload

Overview This command performs the same function as the [reboot](#) command.

show banner external-manager

Overview Use this command to show the current external-manager banner. The external-manager banner warns you that certain features are being managed by an external management system. For example, if you are using Vista Manager EX to manage your network, you will see a notification banner telling you which features are being managed after you enter Global Configuration Mode.

Syntax `show banner external-manager`

Mode User Exec

Example To show the external-manager banner, use the command:

```
awplus# show banner external-manager
```

Output Figure 8-1: Example output from **show banner external-manager**

```
awplus#show banner external-manager
The following features are being managed by external systems.
Configuring these features may have unintended consequences.
Manager: Network Manager
  Feature: ACLs
  Filters

Manager: Vista Manager
  Feature: Traffic control
  Application Priority
  Dynamic Traffic Management
Feature: Web control
  all features
```

Related commands [banner display external-manager](#)
[banner external-manager](#)

Command changes Version 5.5.1-1.1: command added

show clock

Overview This command displays the system's current configured local time and date. It also displays other clock related information such as timezone and summertime configuration.

Syntax show clock

Mode User Exec and Privileged Exec

Example To display the system's current local time, use the command:

```
awplus# show clock
```

Output Figure 8-2: Example output from the **show clock** command for a device using New Zealand time

```
Local Time: Mon, 17 Oct 2016 13:56:06 +1200
UTC Time: Mon, 17 Oct 2016 01:56:06 +0000
Timezone: NZST
Timezone Offset: +12:00
Summer time zone: NZDT
Summer time starts: Last Sunday in September at 02:00:00
Summer time ends: First Sunday in April at 02:00:00
Summer time offset: 60 mins
Summer time recurring: Yes
```

Table 1: Parameters in the output of the **show clock** command

Parameter	Description
Local Time	Current local time.
UTC Time	Current UTC time.
Timezone	The current configured timezone name.
Timezone Offset	Number of hours offset to UTC.
Summer time zone	The current configured summertime zone name.
Summer time starts	Date and time set as the start of summer time.
Summer time ends	Date and time set as the end of summer time.
Summer time offset	Number of minutes that summer time is offset from the system's timezone.
Summer time recurring	Whether the device will apply the summer time settings every year or only once.

Related commands

- [clock summer-time date](#)
- [clock summer-time recurring](#)
- [clock timezone](#)

show cpu

Overview This command displays a list of running processes with their CPU utilization.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show cpu [sort {thrds|pri|sleep|runtime}]`

Parameter	Description
sort	Changes the sorting order using the following fields. If you do not specify a field, then the list is sorted by percentage CPU utilization.
thrds	Sort by the number of threads.
pri	Sort by the process priority.
sleep	Sort by the average time sleeping.
runtime	Sort by the runtime of the process.

Mode User Exec and Privileged Exec

Examples To show the CPU utilization of current processes, sorting them by the number of threads the processes are using, use the command:

```
awplus# show cpu sort thrds
```

Output Figure 8-3: Example output from **show cpu**

```
awplus#show cpu
CPU averages:
 1 second: 0%, 20 seconds: 0%, 60 seconds: 0%
System load averages:
 1 minute: 0.16, 5 minutes: 0.13, 15 minutes: 0.13
Current CPU load:
 userspace: 2%, kernel: 6%, interrupts: 0% iowaits: 0%

user processes
=====
 pid name          thrds  cpu%   pri state sleep% runtime
763 hostd          1    2.9   20  run    0    128
803 diag_monitor   1    0.4   20  sleep  0   3292
768 hsl            14    0.4   20  sleep  0   3912
 1 init            1    0.0   20  sleep  0    686
478 rtccludge      1    0.0   20  sleep  0     9
504 portmap        1    0.0   20  sleep  0     2
17555 sh            1    0.0   20  sleep  0     1
17556 console_log_ale 1    0.0   20  sleep  0     1
515 syslog-ng      1    0.0   20  sleep  0    153
521 dbus-daemon    1    0.0   20  sleep  0     2
532 automount      1    0.0   20  sleep  0    453
571 appmond        1    0.0   20  sleep  0     41
587 crond          1    0.0   20  sleep  0     17
589 openhpid       9    0.0   20  sleep  0    284
609 inetd          1    0.0   20  sleep  0     2
761 nsm            1    0.0   20  sleep  0    260
765 imi            1    0.0   20  sleep  0    616
799 almond         1    0.0   20  sleep  0     52
805 cntrd          1    0.0   20  sleep  0     45
807 poehw          3    0.0   20  sleep  0    207
820 authd          1    0.0   20  sleep  0     76
...

kernel threads
=====
 pid name          cpu%   pri state sleep% runtime
144 aio            0.0    0  sleep  0     0
 95 bdi-default    0.0   20  sleep  0     0
149 crypto         0.0    0  sleep  0     0
474 flush-31:4     0.0   20  sleep  0     1
143 fsnotify_mark  0.0   20  sleep  0     0
426 jffs2_gcd_mtd0 0.0   30  sleep  0    353
 96 kblockd        0.0    0  sleep  0     0
 12 khelper        0.0    0  sleep  0     0
105 khubd          0.0   20  sleep  0     0
 3 ksoftirqd/0     0.0   20  sleep  0     0
142 kswapd0         0.0   20  sleep  0     0
 2 kthreadd        0.0   20  sleep  0     0
 4 kworker/0:0     0.0   20  sleep  0    29
 6 linkwatch       0.0    0  sleep  0     0
466 loop0          0.0    0  sleep  0    801
 7 migration/0     0.0  -100  sleep  0     0
244 mtblock0       0.0   20  sleep  0     5
 93 sync_supers    0.0   20  sleep  0     1
```


Table 2: Parameters in the output of the **show cpu** command

Parameter	Description
CPU averages	Average CPU utilization for the periods stated.
System load averages	The average number of processes waiting for CPU time for the periods stated.
Current CPU load	Current CPU utilization specified by load types.
pid	Identifier number of the process.
name	A shortened name for the process
thrds	Number of threads in the process.
cpu%	Percentage of CPU utilization that this process is consuming.
pri	Process priority state.
state	Process state; one of "run", "sleep", "zombie", and "dead".
sleep%	Percentage of time that the process is in the sleep state.
runtime	The time that the process has been running for, measured in jiffies. A jiffy is the duration of one tick of the system timer interrupt.

**Related
commands**

[show memory](#)
[show memory allocations](#)
[show memory history](#)
[show memory pools](#)
[show process](#)

show cpu history

Overview This command prints a graph showing the historical CPU utilization.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show cpu history`

Mode User Exec and Privileged Exec

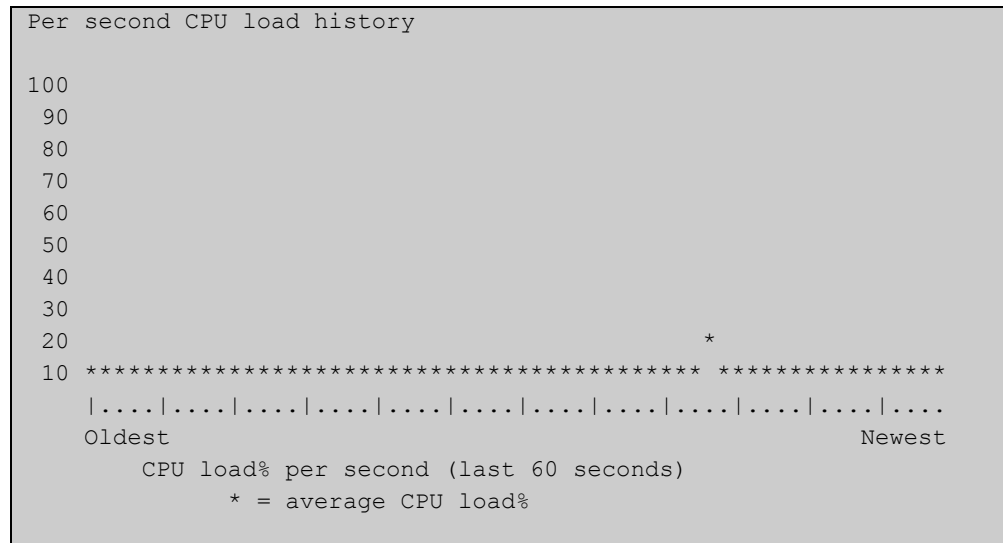
Usage notes This command's output displays three graphs of the percentage CPU utilization:

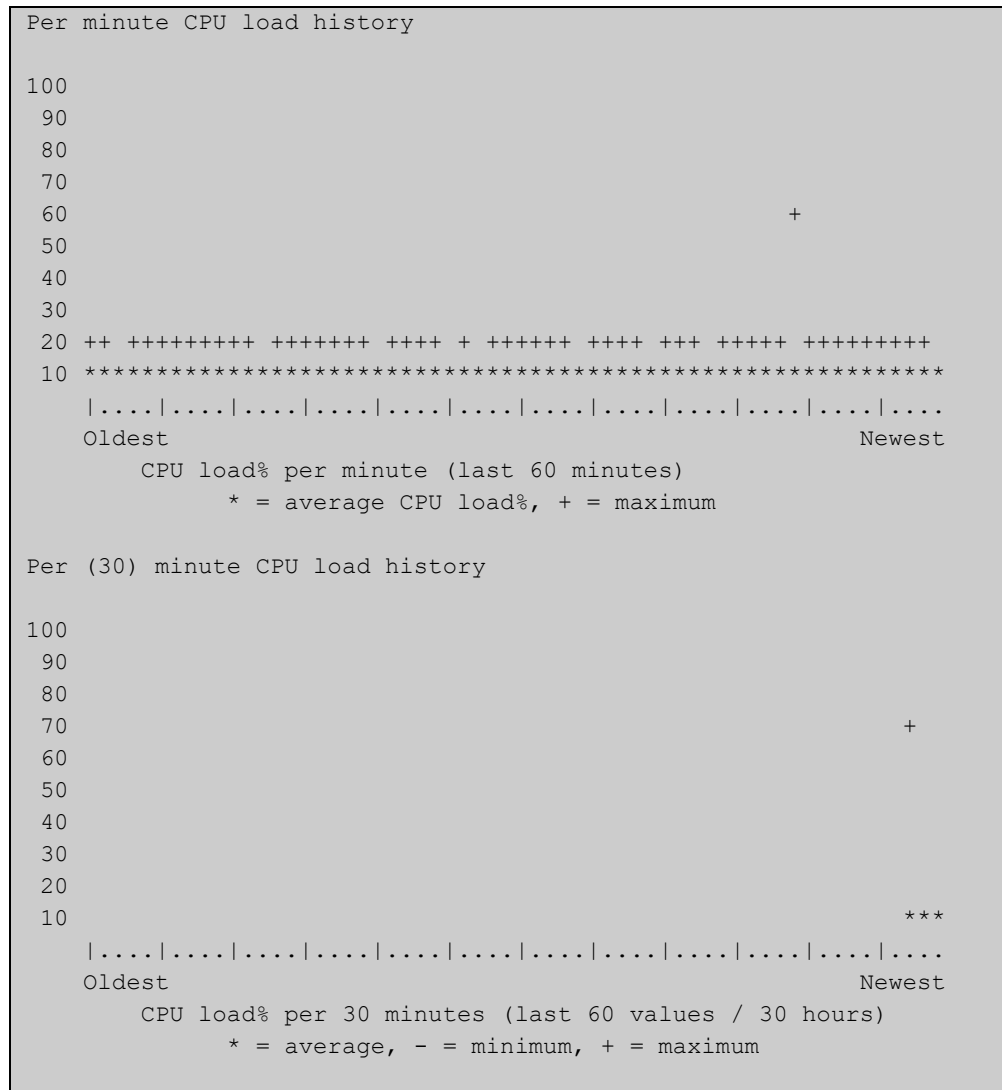
- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

Examples To display a graph showing the historical CPU utilization of the device, use the command:

```
awplus# show cpu history
```

Output Figure 8-4: Example output from the **show cpu history** command





Related commands

- [show memory](#)
- [show memory allocations](#)
- [show memory pools](#)
- [show process](#)

show debugging

Overview This command displays all debugging options in alphabetical order, indicating whether debugging is enabled or disabled for each feature.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax show debugging

Mode User Exec and Privileged Exec

Example To find out what debugging is enabled, use the command:

```
awplus# show debugging
```

Output Figure 8-5: Example output from the **show debugging** command

```
awplus#show debugging
AAA debugging status:
  Authentication debugging is off
  Authorization debugging is off
  Accounting debugging is off
Antivirus Debugging Status: off
% Error: ATMF is not configured.
BGP debugging status:
  BGP debugging is off
  BGP nht debugging is off
  BGP nsm debugging is off
  BGP events debugging is off
  BGP keepalives debugging is off
  BGP updates debugging is off
  BGP fsm debugging is off
  BGP filter debugging is off
  BGP Route Flap Dampening debugging is off

Firewall Debugging Status: off
Traffic shaping debugging status: off
IGMP Debugging status:
  IGMP Decoder debugging is off
  IGMP Encoder debugging is off
  IGMP Events debugging is off
  IGMP FSM debugging is off
  IGMP Tree-Info-Base (TIB) debugging is off
DNS Relay debugging status:
  debugging is off
IP packet debugging status:
OSPFv3 debugging status:
...
```

show memory

Overview This command displays the memory used by each process that is currently running.

For information on filtering and saving command output, see the [Getting Started with the AlliedWare Plus Command Line Interface](#).

Syntax `show memory [sort {size|peak|stk}]`

Parameter	Description
sort	Changes the sorting order for the list of processes. If you do not specify this, then the list is sorted by percentage memory utilization.
	size Sort by the amount of memory the process is currently using.
	peak Sort by the greatest amount of memory ever used by the process.
	stk Sort by the stack size of the process.

Mode User Exec and Privileged Exec

Example To display the memory used by the current running processes, use the command:

```
awplus# show memory
```

Output Figure 8-6: Example output from **show memory**

```
awplus#show memory
```

RAM total: 824680 kB; free: 635032 kB; buffers: 20272 kB						
user processes						
=====						
pid	name	mem%	size (kB)	peak (kB)	data (kB)	virt (kB)
1443	squid	1.9	16408	299768	23568	299768
1441	squid	1.9	16416	299776	23568	299776
1440	squid	1.9	16416	299776	23568	299776
1439	squid	1.9	16416	299776	23568	299776
1438	squid	1.9	16152	298928	23568	298864
1226	imi	1.3	10968	23104	2760	22912
1228	hsl	1.2	10512	692944	608160	631856
2156	imish	1.0	8856	158456	75904	94696
1221	nsm	1.0	9008	21696	1968	21632
1296	ospfd	0.8	6936	19144	1016	19080
1293	bgpd	0.8	7264	19184	1168	19120
1291	pimd	0.8	6600	20992	2944	20928
1283	ripd	0.8	6640	18328	944	18256
...						

Table 3: Parameters in the output of the **show memory** command

Parameter	Description
RAM total	Total amount of RAM memory free.
free	Available memory size.
buffers	Memory allocated kernel buffers.
pid	Identifier number for the process.
name	Short name used to describe the process.
mem%	Percentage of memory utilization the process is currently using.
size	Amount of memory currently used by the process.
peak	Greatest amount of memory ever used by the process.
data	Amount of memory used for data.
stk	The stack size.

Related commands

- [low-memory restart](#)
- [show memory allocations](#)
- [show memory history](#)
- [show memory pools](#)
- [show memory shared](#)
- [snmp-server enable trap low-memory](#)

show memory allocations

Overview This command displays the memory allocations used by processes.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show memory allocations [<process>]`

Parameter	Description
<process>	Displays the memory allocation used by the specified process.

Mode User Exec and Privileged Exec

Example To display the memory allocations used by all processes on your device, use the command:

```
awplus# show memory allocations
```

Output Figure 8-7: Example output from the **show memory allocations** command

```
awplus#show memory allocations
Memory allocations for imi
-----

Current 15093760 (peak 15093760)

Statically allocated memory:
- binary/exe           :    1675264
- libraries            :    8916992
- bss/global data      :    2985984
- stack                :    139264

Dynamically allocated memory (heap):
- total allocated       :    1351680
- in use                :    1282440
- non-mmapped           :    1351680
- maximum total allocated :    1351680
- total free space      :     69240
- releasable            :     68968
- space in freed fastbins :        16

Context
      filename:line    allocated    freed
+      lib.c:749        484
.
.
.
```

**Related
commands**

- [show memory](#)
- [show memory history](#)
- [show memory pools](#)
- [show memory shared](#)
- [show tech-support](#)

show memory history

Overview This command prints a graph showing the historical memory usage.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show memory history`

Mode User Exec and Privileged Exec

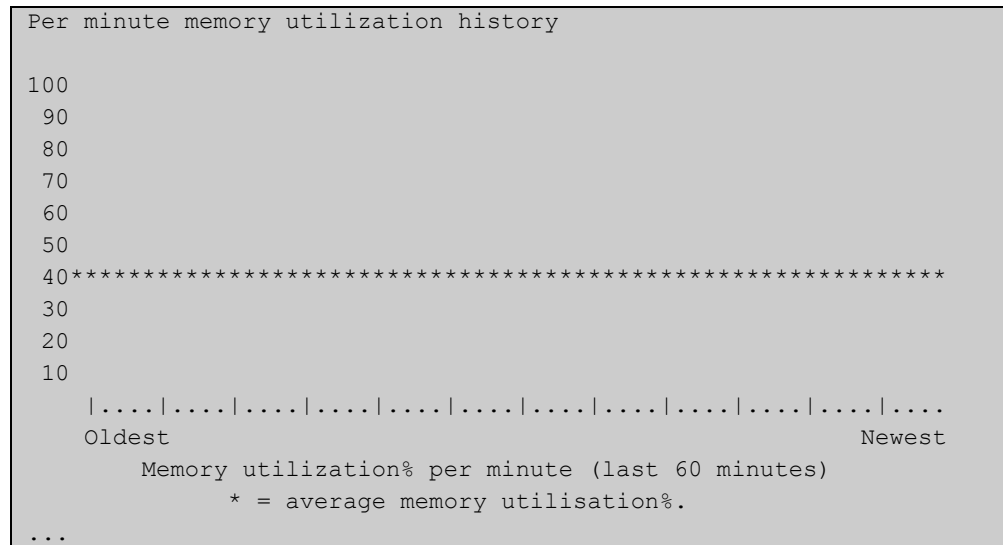
Usage notes This command’s output displays three graphs of the percentage memory utilization:

- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

Examples To show a graph displaying the historical memory usage, use the command:

```
awplus# show memory history
```

Output Figure 8-8: Example output from the **show memory history** command



Related commands

- [show memory allocations](#)
- [show memory pools](#)
- [show memory shared](#)
- [show tech-support](#)

show memory pools

Overview This command shows the memory pools used by processes.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show memory pools [<process>]`

Parameter	Description
<process>	Displays the memory pools used by the specified process.

Mode User Exec and Privileged Exec

Example To show the memory pools used by processes, use the command:

```
awplus# show memory pools
```

Output Figure 8-9: Example output from the **show memory pools** command

```
awplus#show memory pools
Memory pools for imi
-----

Current 15290368 (peak 15290368)

Statically allocated memory:
- binary/exe           : 1675264
- libraries            : 8916992
- bss/global data     : 2985984
- stack                : 139264

Dynamically allocated memory (heap):
- total allocated      : 1548288
- in use               : 1479816
- non-mmapped         : 1548288
- maximum total allocated : 1548288
- total free space     : 68472
- releasable          : 68200
- space in freed fastbins : 16
.
.
.
```

Related commands

- [show memory allocations](#)
- [show memory history](#)
- [show tech-support](#)

show memory shared

Overview This command displays shared memory allocation information. The output is useful for diagnostic purposes by Allied Telesis authorized service personnel.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show memory shared`

Mode User Exec and Privileged Exec

Example To display information about the shared memory allocation used on the device, use the command:

```
awplus# show memory shared
```

Output Figure 8-10: Example output from the **show memory shared** command

```
awplus#show memory shared
Shared Memory Status
-----
Segment allocated   = 39
Pages allocated     = 39
Pages resident      = 11

Shared Memory Limits
-----
Maximum number of segments           = 4096
Maximum segment size (kbytes)        = 32768
Maximum total shared memory (pages)  = 2097152
Minimum segment size (bytes)         = 1
```

Related commands

- [show memory allocations](#)
- [show memory history](#)
- [show memory](#)

show process

Overview This command lists a summary of the current running processes.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show process [sort {cpu|mem}]`

Parameter	Description
sort	Changes the sorting order for the list of processes.
cpu	Sorts the list by the percentage of CPU utilization.
mem	Sorts the list by the percentage of memory utilization.

Mode User Exec and Privileged Exec

Usage notes This command displays a snapshot of currently-running processes. If you want to see CPU or memory utilization history instead, use the commands [show cpu history](#) or [show memory history](#).

Example To display a summary of the current running processes, use the command:

```
awplus# show process
```

Output Figure 8-11: Example output from the **show process** command

```
CPU averages:
 1 second: 8%, 20 seconds: 5%, 60 seconds: 5%
System load averages:
 1 minute: 0.04, 5 minutes: 0.08, 15 minutes: 0.12
Current CPU load:
 userspace: 9%, kernel: 9%, interrupts: 0% iowaits: 0%
RAM total: 514920 kB; free: 382600 kB; buffers: 16368 kB

user processes
=====
pid name      thrds  cpu%  mem%   pri  state  sleep%
962 pss        12    0     6    25  sleep    5
1  init         1     0     0    25  sleep    0
797 syslog-ng   1     0     0    16  sleep   88
...
kernel threads
=====
pid name      cpu%  pri  state  sleep%
71  aio/0      0    20  sleep    0
3  events/0   0    10  sleep   98
...
```

Table 4: Parameters in the output from the **show process** command

Parameter	Description
CPU averages	Average CPU utilization for the periods stated.
System load averages	The average number of processes waiting for CPU time for the periods stated.
Current CPU load	Current CPU utilization specified by load types
RAM total	Total memory size.
free	Available memory.
buffers	Memory allocated to kernel buffers.
pid	Identifier for the process.
name	Short name to describe the process.
thrds	Number of threads in the process.
cpu%	Percentage of CPU utilization that this process is consuming.
mem%	Percentage of memory utilization that this process is consuming.
pri	Process priority.
state	Process state; one of "run", "sleep", "stop", "zombie", or "dead".
sleep%	Percentage of time the process is in the sleep state.

Related commands [show cpu](#)
[show cpu history](#)

show reboot history

Overview Use this command to display the device's reboot history.

Syntax `show reboot history`

Mode User Exec and Privileged Exec

Example To show the reboot history, use the command:

```
awplus# show reboot history
```

Output Figure 8-12: Example output from the **show reboot history** command

```
awplus#show reboot history
```

<date>	<time>	<type>	<description>
2016-10-10	01:42:04	Expected	User Request
2016-10-10	01:35:31	Expected	User Request
2016-10-10	01:16:25	Unexpected	Rebooting due to critical process (network/nsm) failure!
2016-10-10	01:11:04	Unexpected	Rebooting due to critical process (network/nsm) failure!
2016-10-09	19:56:16	Expected	User Request
2016-10-09	19:51:20	Expected	User Request

Table 5: Parameters in the output from the **show reboot history** command

Parameter	Description
Unexpected	A non-intended reboot.
Expected	A planned or user-triggered reboot.
User request	User initiated reboot via the CLI.

Related commands [show tech-support](#)

show router-id

Overview Use this command to show the Router ID of the current system.

Syntax `show router-id`

Mode User Exec and Privileged Exec

Example To display the Router ID of the current system, use the command:

```
awplus# show router-id
```

Output Figure 8-13: Example output from the **show router-id** command

```
awplus>show router-id  
Router ID: 10.55.0.2 (automatic)
```

show system

Overview Use this command to display general system information about the device, including the hardware, memory usage, and software version. It also displays location and contact details when these have been set.

For information on filtering and saving command output, see the [Getting Started with the AlliedWare Plus Command Line Interface](#).

Syntax `show system`

Mode User Exec and Privileged Exec

Example To display configuration information, use the command:

```
awplus# show system
```

Output Figure 8-14: Example output from **show system**

```
awplus#show system
System Status                                     Web Feb 16 10:32:16 2022

Board      ID   Bay   Board Name                      Rev   Serial number
-----
Base       600  Base   AT-vFW                          A-0   CB0B8934FBBD43BC
-----

RAM: Total: 32782560 kB Free: 32650576 kB
Flash: 968.3MB Used: 19.9MB Available: 882.3MB
-----

Uptime                : 3 days 19:18:11

Current software      : vfw_x86_64-5.5.1-2.1.rel
Software version      : 5.5.1-2.1
Build date            : Tue Nov 30 18:35:55 UTC 2022
Current boot config: flash:/default.cfg (file exists)

System Name
awplus
System Contact
System Location
-----
```


show system mac

Overview This command displays the physical MAC address of the device.

Syntax `show system mac`

Mode User Exec and Privileged Exec

Example To display the physical MAC address enter the following command:

```
awplus# show system mac
```

Output Figure 8-15: Example output from the **show system mac** command

```
awplus#show system mac
0200.0034.5682 (eth1)
0200.0034.5683 (eth2)
0200.0034.5684 (system)
```

show system serialnumber

Overview This command shows the serial number information for the device.
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show system serialnumber`

Mode User Exec and Privileged Exec

Example To display the serial number information for the device, use the command:

```
awplus# show system serialnumber
```

Output Figure 8-16: Example output from the **show system serialnumber** command

```
awplus#show system serialnumber
45AX5300X
```

show tech-support

Overview This command generates system and debugging information for the device and saves it to a file.

This command is useful for collecting a large amount of information so that it can then be analyzed for troubleshooting purposes. The output of this command can be provided to technical support staff when reporting a problem.

You can optionally limit the command output to display only information for a given protocol or feature. The features available depend on your device and will be a subset of the features listed in the table below.

Syntax `show tech-support`
{ [all|atmf|auth|bgp|card|dhcpsn|epsr|firewall|igmp|ip|ipv6|mld|openflow|ospf|ospf6|pim|rip|ripng|stack|stp|system|tacacs+|update]} [outfile <filename>]

Parameter	Description
all	Display full information
atmf	Display ATMF-specific information
auth	Display authentication-related information
bgp	Display BGP-related information
card	Display Chassis Card specific information
dhcpsn	Display DHCP Snooping specific information
epsr	Display EPSR specific information
firewall	Display firewall specific information
igmp	Display IGMP specific information
ip	Display IP specific information
ipv6	Display IPv6 specific information
mld	Display MLD specific information
openflow	Display information related to OpenFlow
ospf	Display OSPF related information
ospf6	Display OSPF6 specific information
pim	Display PIM related information
rip	RIP related information
ripng	Display RIPNG specific information
stack	Display stacking device information
stp	Display STP specific information
system	Display general system information

Parameter	Description
tacacs+	Display TACACS+ information
update	Display resource update specific information
	Output modifier
>	Output redirection
>>	Output redirection (append)
outfile	Output file name
<filename>	Specifies a name for the output file. If no name is specified, this file will be saved as: tech-support.txt.gz.

Default Captures **all** information for the device.

By default the output is saved to the file 'tech-support.txt.gz' in the current directory. If this file already exists in the current directory then a new file is generated with the time stamp appended to the file name, for example 'tech-support20161009.txt.gz', so the previous file is retained.

Usage notes The command generates a large amount of output, which is saved to a file in compressed format. The output file name can be specified by outfile option. If the output file already exists, a new file name is generated with the current time stamp. If the output filename does not end with ".gz", then ".gz" is appended to the filename. Since output files may be too large for Flash on the device we recommend saving files to external memory or a TFTP server whenever possible to avoid device lockup. This method is not likely to be appropriate when running the working set option of AMF across a range of physically separated devices.

Mode Privileged Exec

Examples To produce the output needed by technical support staff, use the command:

```
awplus# show tech-support
```

terminal monitor

Overview Use this command to display debugging output on a terminal.

To display the cursor after a line of debugging output, press the Enter key.

Use the command **terminal no monitor** or **no terminal monitor** to stop displaying debugging output on the terminal. Alternatively, you can use the timeout option to stop displaying debugging output on the terminal after a set time.

Syntax terminal monitor [<1-60>]
terminal no monitor
no terminal monitor

Parameter	Description
<1-60>	Set a timeout between 1 and 60 seconds for terminal output.

Default Disabled

Mode User Exec and Privileged Exec

Examples To display debugging output on a terminal, enter the command:

```
awplus# terminal monitor
```

To display debugging on the terminal for 60 seconds, enter the command:

```
awplus# terminal monitor 60
```

To stop displaying debugging output on the terminal, use the command:

```
awplus# no terminal monitor
```

Related commands All debug commands

Command changes Version 5.4.8-0.2: **no terminal monitor** added as an alias for **terminal no monitor**

undebbug all

Overview This command applies the functionality of the `no debbug all` command.

9

Logging Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure logging. See the [Logging Feature Overview and Configuration Guide](#) for more information about the different types of log and how to filter log messages.

- Command List**
- [“clear exception log”](#) on page 293
 - [“clear log”](#) on page 294
 - [“clear log buffered”](#) on page 295
 - [“clear log permanent”](#) on page 296
 - [“connection-log events”](#) on page 297
 - [“copy buffered-log”](#) on page 298
 - [“copy permanent-log”](#) on page 299
 - [“default log buffered”](#) on page 300
 - [“default log console”](#) on page 301
 - [“default log email”](#) on page 302
 - [“default log host”](#) on page 303
 - [“default log monitor”](#) on page 304
 - [“default log permanent”](#) on page 305
 - [“log buffered”](#) on page 306
 - [“log buffered \(filter\)”](#) on page 307
 - [“log buffered exclude”](#) on page 310
 - [“log buffered size”](#) on page 313
 - [“log console”](#) on page 314
 - [“log console \(filter\)”](#) on page 315

- ["log console exclude"](#) on page 318
- ["log date-format"](#) on page 321
- ["log email"](#) on page 322
- ["log email \(filter\)"](#) on page 323
- ["log email exclude"](#) on page 326
- ["log email time"](#) on page 329
- ["log facility"](#) on page 331
- ["log host"](#) on page 333
- ["log host \(filter\)"](#) on page 335
- ["log host exclude"](#) on page 338
- ["log host source"](#) on page 341
- ["log host startup-delay"](#) on page 342
- ["log host time"](#) on page 344
- ["log monitor \(filter\)"](#) on page 346
- ["log monitor exclude"](#) on page 349
- ["log permanent"](#) on page 352
- ["log permanent \(filter\)"](#) on page 353
- ["log permanent exclude"](#) on page 356
- ["log permanent size"](#) on page 359
- ["log-rate-limit nsm"](#) on page 360
- ["log trustpoint"](#) on page 361
- ["log url-requests"](#) on page 362
- ["show connection-log events"](#) on page 363
- ["show counter log"](#) on page 364
- ["show exception log"](#) on page 365
- ["show log"](#) on page 366
- ["show log config"](#) on page 368
- ["show log permanent"](#) on page 370
- ["show running-config log"](#) on page 372

clear exception log

Overview This command resets the contents of the exception log, but does not remove the associated core files.

Syntax `clear exception log`

Mode Privileged Exec

Example `awplus# clear exception log`

clear log

Overview This command removes the contents of the buffered and permanent logs.

Syntax `clear log`

Mode Privileged Exec

Example To delete the contents of the buffered and permanent log use the command:

```
awplus# clear log
```

Related commands

- [clear log buffered](#)
- [clear log permanent](#)
- [show log](#)

clear log buffered

Overview This command removes the contents of the buffered log.

Syntax `clear log buffered`

Mode Privileged Exec

Example To delete the contents of the buffered log use the following commands:

```
awplus# clear log buffered
```

Related commands

- [default log buffered](#)
- [log buffered](#)
- [log buffered \(filter\)](#)
- [log buffered size](#)
- [log buffered exclude](#)
- [show log](#)
- [show log config](#)

clear log permanent

Overview This command removes the contents of the permanent log.

Syntax clear log permanent

Mode Privileged Exec

Example To delete the contents of the permanent log use the following commands:

```
awplus# clear log permanent
```

Related commands

- default log permanent
- log permanent
- log permanent (filter)
- log permanent exclude
- log permanent size
- show log config
- show log permanent

connection-log events

Overview Use this command to enable extra logging for indicating the start and the end of connections passing through the firewall.

Use the **no** variant of this command to turn off the extra logging of connections passing through the firewall.

Syntax `connection-log events [new|end|all]`
`no connection-log events [new|end|all]`

Parameter	Description
new	New connection
end	Connections closed
all	All new connections and connections closed. Default.

Default Connection logging is not enabled by default.

Mode Global Configuration.

Usage notes There are two types of messages you can log: new connections and connections that ended. You can control the amount of messages you log by choosing to log either type of message or all of the message types.

Messages contain the following information:

- time
- source and destination addresses (NATed and unNATed)
- protocol
- source and destination ports (NATed and unNATed)
- bytes and packets passed (found in the connection end message)

Example To log all of the new connections and all of the closed connections, use the commands:

```
awplus# configure terminal
awplus(config)# connection-log events all
```

Related commands [show connection-log events](#)

Command changes Version 5.4.7-1.1: command added.

copy buffered-log

Overview Use this command to copy the buffered log to an internal or external destination.

Syntax `copy buffered-log <destination-name>`

Parameter	Description
<code><destination-name></code>	The filename and path for the destination file. See Introduction on page 120 for valid syntax.

Mode Privileged Exec

Example To copy the buffered log file into a folder in Flash named “buffered-log” and name the file “buffered-log.log”, use the command:

```
awplus# copy buffered-log flash:/buffered-log/buffered-log.log
```

Related commands

- [log buffered](#)
- [show file systems](#)
- [show log](#)

Command changes Version 5.4.7-1.1: command added

copy permanent-log

Overview Use this command to copy the permanent log to an internal or external destination.

Syntax `copy permanent-log <destination-name>`

Parameter	Description
<code><destination-name></code>	The filename and path for the destination file. See Introduction on page 120 for valid syntax.

Mode Privileged Exec

Example To copy the permanent log file into a folder in Flash named “perm-log” and name the file “permanent-log.log”, use the command:

```
awplus# copy permanent-log flash:/perm-log/permanent-log.log
```

Related commands

- [log permanent](#)
- [show file systems](#)
- [show log permanent](#)

Command changes Version 5.4.7-1.1: command added

default log buffered

Overview This command restores the default settings for the buffered log stored in RAM. By default the size of the buffered log is 50 kB and it accepts messages with the severity level of “warnings” and above.

Syntax `default log buffered`

Default The buffered log is enabled by default.

Mode Global Configuration

Example To restore the buffered log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log buffered
```

Related commands

- [clear log buffered](#)
- [log buffered](#)
- [log buffered \(filter\)](#)
- [log buffered size](#)
- [log buffered exclude](#)
- [show log](#)
- [show log config](#)

default log console

Overview This command restores the default settings for log messages sent to the terminal when a [log console](#) command is issued. By default all messages are sent to the console when a **log console** command is issued.

Syntax `default log console`

Mode Global Configuration

Example To restore the log console to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log console
```

Related commands

- [log console](#)
- [log console \(filter\)](#)
- [log console exclude](#)
- [show log config](#)

default log email

Overview This command restores the default settings for log messages sent to an email address. By default no filters are defined for email addresses. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax `default log email <email-address>`

Parameter	Description
<code><email-address></code>	The email address to send log messages to

Mode Global Configuration

Example To restore the default settings for log messages sent to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# default log email admin@alliedtelesis.com
```

Related commands

- [log email](#)
- [log email \(filter\)](#)
- [log email exclude](#)
- [log email time](#)
- [show log config](#)

default log host

Overview This command restores the default settings for log sent to a remote syslog server. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax `default log host <ip-addr>`

Parameter	Description
<code><ip-addr></code>	The IP address of a remote syslog server

Mode Global Configuration

Example To restore the default settings for messages sent to the remote syslog server with IP address 10.32.16.21 use the following commands:

```
awplus# configure terminal
awplus(config)# default log host 10.32.16.21
```

Related commands

- [log host](#)
- [log host \(filter\)](#)
- [log host exclude](#)
- [log host source](#)
- [log host time](#)
- [show log config](#)

default log monitor

Overview This command restores the default settings for log messages sent to the terminal when a [terminal monitor](#) command is used.

Syntax `default log monitor`

Default All messages are sent to the terminal when a [terminal monitor](#) command is used.

Mode Global Configuration

Example To restore the log monitor to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log monitor
```

Related commands

- [log monitor \(filter\)](#)
- [log monitor exclude](#)
- [show log config](#)
- [terminal monitor](#)

default log permanent

Overview This command restores the default settings for the permanent log stored in NVS. By default, the size of the permanent log is 50 kB and it accepts messages with the severity level of `warnings` and above.

Syntax `default log permanent`

Default The permanent log is enabled by default.

Mode Global Configuration

Example To restore the permanent log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log permanent
```

Related commands

- `clear log permanent`
- `log permanent`
- `log permanent (filter)`
- `log permanent exclude`
- `log permanent size`
- `show log config`
- `show log permanent`

log buffered

Overview This command configures the device to store log messages in RAM. Messages stored in RAM are not retained on the device over a restart. Once the buffered log reaches its configured maximum allowable size old messages will be deleted to make way for new ones.

Syntax `log buffered`
`no log buffered`

Default The buffered log is configured by default.

Mode Global Configuration

Examples To configured the device to store log messages in RAM use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered
```

To configure the device to not store log messages in a RAM buffer use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered
```

Related commands

- [clear log buffered](#)
- [copy buffered-log](#)
- [default log buffered](#)
- [log buffered \(filter\)](#)
- [log buffered size](#)
- [log buffered exclude](#)
- [show log](#)
- [show log config](#)

log buffered (filter)

Overview Use this command to create a filter to select messages to be sent to the buffered log. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the buffered log.

Syntax `log buffered [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`
`no log buffered [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

Parameter	Description
level	Filter messages to the buffered log by severity level.
<level>	The minimum severity of message to send to the buffered log. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:
0 emergencies	System is unusable
1 alerts	Action must be taken immediately
2 critical	Critical conditions
3 errors	Error conditions
4 warnings	Warning conditions
5 notices	Normal, but significant, conditions
6 informational	Informational messages
7 debugging	Debug-level messages
program	Filter messages to the buffered log by program. Include messages from a specified program in the buffered log.
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.
rip	Routing Information Protocol (RIP)
ripng	Routing Information Protocol - next generation (RIPng)
ospf	Open Shortest Path First (OSPF)
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)
bgp	Border Gateway Protocol (BGP)
rsvp	Resource Reservation Protocol (RSVP)
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)

Parameter	Description
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpcsn	DHCP snooping (DHCP SN)
facility	Filter messages to the buffered log by syslog facility.
<facility>	Specify one of the following syslog facilities to include messages from in the buffered log:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Select messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default By default the buffered log has a filter to select messages whose severity level is “notices (5)” or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To add a filter to send all messages containing the text “Bridging initialization” to the buffered log, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# log buffered msgtext Bridging initialization
```

To remove a filter that sends all messages containing the text “Bridging initialization” to the buffered log, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no log buffered msgtext Bridging initialization
```

Related commands

- [clear log buffered](#)
- [default log buffered](#)
- [log buffered](#)
- [log buffered size](#)
- [log buffered exclude](#)
- [show log](#)
- [show log config](#)

log buffered exclude

Overview Use this command to exclude specified log messages from the buffered log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax `log buffered exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log buffered exclude [level <level>] [program
<program-name>] [facility <facility>] [msgtext <text-string>]`

Parameter	Description
level	Exclude messages of the specified severity level.
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:
0 emergencies	System is unusable
1 alerts	Action must be taken immediately
2 critical	Critical conditions
3 errors	Error conditions
4 warnings	Warning conditions
5 notices	Normal, but significant, conditions
6 informational	Informational messages
7 debugging	Debug-level messages
program	Exclude messages from a specified program.
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.
rip	Routing Information Protocol (RIP)
ripng	Routing Information Protocol - next generation (RIPng)
ospf	Open Shortest Path First (OSPF)
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)
bgp	Border Gateway Protocol (BGP)

Parameter	Description
rsvp	Resource Reservation Protocol (RSVP)
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpcsn	DHCP snooping (DHPCPSN)
facility	Exclude messages from a syslog facility.
<facility>	Specify one of the following syslog facilities to exclude messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Exclude messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered exclude msgtext example of
irrelevant message
```

Related commands

- clear log buffered
- default log buffered
- log buffered
- log buffered (filter)
- log buffered size
- show log
- show log config

log buffered size

Overview This command configures the amount of memory that the buffered log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

Use the **no** variant of this command to return to the default.

Syntax `log buffered size <50-250>`
`no log buffered size`

Parameter	Description
<50-250>	Size of the RAM log in kilobytes

Default 50 kilobytes

Mode Global Configuration

Example To allow the buffered log to use up to 100 kilobytes of RAM, use the commands:

```
awplus# configure terminal
awplus(config)# log buffered size 100
```

To return to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no log buffered size
```

Related commands

- [clear log buffered](#)
- [copy buffered-log](#)
- [default log buffered](#)
- [log buffered](#)
- [log buffered \(filter\)](#)
- [log buffered exclude](#)
- [show log](#)
- [show log config](#)

log console

Overview This command configures the device to send log messages to consoles. The console log is configured by default to send messages to the device's main console port.

Use the **no** variant of this command to configure the device not to send log messages to consoles.

Syntax `log console`
`no log console`

Mode Global Configuration

Examples To configure the device to send log messages use the following commands:

```
awplus# configure terminal
awplus(config)# log console
```

To configure the device not to send log messages in all consoles use the following commands:

```
awplus# configure terminal
awplus(config)# no log console
```

Related commands [default log console](#)
[log console \(filter\)](#)
[log console exclude](#)
[show log config](#)

log console (filter)

Overview This command creates a filter to select messages to be sent to all consoles when the **log console** command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

Syntax `log console [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`
`no log console [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

Parameter	Description
level	Filter messages by severity level.
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:
0 emergencies	System is unusable
1 alerts	Action must be taken immediately
2 critical	Critical conditions
3 errors	Error conditions
4 warnings	Warning conditions
5 notices	Normal, but significant, conditions
6 informational	Informational messages
7 debugging	Debug-level messages
program	Filter messages by program. Include messages from a specified program.
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.
rip	Routing Information Protocol (RIP)
ripng	Routing Information Protocol - next generation (RIPng)
ospf	Open Shortest Path First (OSPF)
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)
bgp	Border Gateway Protocol (BGP)
rsvp	Resource Reservation Protocol (RSVP)
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)

Parameter	Description
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpcsn	DHCP snooping (DHPCPSN)
facility	Filter messages by syslog facility.
<facility>	Specify one of the following syslog facilities to include messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Select messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default By default the console log has a filter to select messages whose severity level is **critical** or higher. This filter may be removed using the **no** variant of this command. This filter may be removed and replaced by filters that are more selective.

Mode Global Configuration

Examples To create a filter to send all messages containing the text "Bridging initialization" to console instances where the **log console** command has been entered, use the following commands:

```
awplus# configure terminal
awplus(config)# log console msgtext "Bridging initialization"
```

To remove a default filter that includes sending **critical**, **alert** and **emergency** level messages to the console, use the following commands:

```
awplus# configure terminal
awplus(config)# no log console level critical
```

Related commands

- [default log console](#)
- [log console](#)
- [log console exclude](#)
- [show log config](#)

log console exclude

Overview Use this command to prevent specified log messages from being sent to the console, when console logging is turned on. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax `log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]`
`no log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]`

Parameter	Description
level	Exclude messages of the specified severity level.
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:
0 emergencies	System is unusable
1 alerts	Action must be taken immediately
2 critical	Critical conditions
3 errors	Error conditions
4 warnings	Warning conditions
5 notices	Normal, but significant, conditions
6 informational	Informational messages
7 debugging	Debug-level messages
program	Exclude messages from a specified program.
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.
rip	Routing Information Protocol (RIP)
ripng	Routing Information Protocol - next generation (RIPng)
ospf	Open Shortest Path First (OSPF)
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)

Parameter	Description
bgp	Border Gateway Protocol (BGP)
rsvp	Resource Reservation Protocol (RSVP)
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (DHCP SN)
facility	Exclude messages from a syslog facility.
<facility>	Specify one of the following syslog facilities to exclude messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon

Parameter	Description
msgtext	Exclude messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log console exclude msgtext example of
irrelevant message
```

Related commands

- [default log console](#)
- [log console](#)
- [log console \(filter\)](#)
- [show log config](#)

log date-format

Overview Use this command to change the date format for log messages to an ISO 8601 compliant format, or to return to the default date format.

Syntax `log date-format {iso|default}`

Parameter	Description
iso	Display the date and time in the ISO 8601 compliant format of: YYYY-MM-DDThh:mm:ssTZD
default	Display the date and time in the default date format of YYYY MMM DD HH:MM:SS

Default The default option of YYYY MMM DD HH:MM:SS (except when using terminal monitor, when it is HH:MM:SS)

Mode Global Configuration

Usage notes In the ISO 8601 compliant format, a T separates the date from the time, and the time is followed by the timezone offset from UTC time. For example, this is a log message with an ISO 8601 compliant date:

```
2016-09-29T08:55:43+13:00 user.notice Gateway IMISH[1983]:  
[manager@ttyS0]show run
```

This is a log message with the default date format:

```
2016 Sep 29 08:55:43 user.notice Gateway IMISH[1983]:  
[manager@ttyS0]show run
```

The date format setting affects all log messages, no matter where the messages are stored or displayed.

Examples To set the date format to the ISO 8601 compliant format, use the commands:

```
awplus# configure terminal  
awplus(config)# log date-format iso
```

To return to the default date format of YYYY MMM DD HH:MM:SS, use the commands:

```
awplus# configure terminal  
awplus(config)# log date-format default
```

Related commands [show exception log](#)
[show log](#)
[show log permanent](#)

Command changes Version 5.4.6-2.1: command added

log email

Overview This command configures the device to send log messages to an email address. The email address is specified in this command.

Syntax `log email <email-address>`

Parameter	Description
<code><email-address></code>	The email address to send log messages to

Default By default no filters are defined for email log targets. Filters must be defined before messages will be sent.

Mode Global Configuration

Example To have log messages emailed to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com
```

Related commands

- [default log email](#)
- [log email \(filter\)](#)
- [log email exclude](#)
- [log email time](#)
- [show log config](#)

log email (filter)

Overview This command creates a filter to select messages to be sent to an email address. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a specified email address. All configuration relating to this log target will be removed.

Syntax `log email <email-address> [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`
`no log email <email-address> [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

Parameter	Description																
<code><email-address></code>	The email address to send logging messages to																
<code>level</code>	Filter messages by severity level.																
<code><level></code>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	0 emergencies	System is unusable	1 alerts	Action must be taken immediately	2 critical	Critical conditions	3 errors	Error conditions	4 warnings	Warning conditions	5 notices	Normal, but significant, conditions	6 informational	Informational messages	7 debugging	Debug-level messages
0 emergencies	System is unusable																
1 alerts	Action must be taken immediately																
2 critical	Critical conditions																
3 errors	Error conditions																
4 warnings	Warning conditions																
5 notices	Normal, but significant, conditions																
6 informational	Informational messages																
7 debugging	Debug-level messages																
<code>program</code>	Filter messages by program. Include messages from a specified program.																
<code><program-name></code>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)						
rip	Routing Information Protocol (RIP)																
ripng	Routing Information Protocol - next generation (RIPng)																
ospf	Open Shortest Path First (OSPF)																
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																
bgp	Border Gateway Protocol (BGP)																

Parameter	Description
rsvp	Resource Reservation Protocol (RSVP)
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpcsn	DHCP snooping (DHCP SN)
facility	Filter messages by syslog facility.
<facility>	Specify one of the following syslog facilities to include messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Select messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Mode Global Configuration

Examples To create a filter to send all messages containing the text "Bridging initialization", to the email address admin@homebase.com, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@homebase.com msgtext "Bridging
initialization"
```

To create a filter to send messages with a severity level of **informational** and above to the email address admin@alliedtelesis.com, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com level
informational
```

To stop the device emailing log messages emailed to the email address admin@alliedtelesis.com, use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@homebase.com
```

To remove a filter that sends messages with a severity level of **informational** and above to the email address admin@alliedtelesis.com, use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@alliedtelesis.com level
informational
```

Related commands

- [default log email](#)
- [log email](#)
- [log email exclude](#)
- [log email time](#)
- [show log config](#)

log email exclude

Overview Use this command to prevent specified log messages from being emailed, when the device is configured to send log messages to an email address. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax `log email exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]`
`no log email exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]`

Parameter	Description
level	Exclude messages of the specified severity level.
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:
0 emergencies	System is unusable
1 alerts	Action must be taken immediately
2 critical	Critical conditions
3 errors	Error conditions
4 warnings	Warning conditions
5 notices	Normal, but significant, conditions
6 informational	Informational messages
7 debugging	Debug-level messages
program	Exclude messages from a specified program.
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.
rip	Routing Information Protocol (RIP)
ripng	Routing Information Protocol - next generation (RIPng)
ospf	Open Shortest Path First (OSPF)
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)

Parameter	Description
bgp	Border Gateway Protocol (BGP)
rsvp	Resource Reservation Protocol (RSVP)
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (DHCP SN)
facility	Exclude messages from a syslog facility.
<facility>	Specify one of the following syslog facilities to exclude messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon

Parameter	Description
msgtext	Exclude messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# log email exclude msgtext example of irrelevant  
message
```

**Related
commands**

- [default log email](#)
- [log email](#)
- [log email \(filter\)](#)
- [log email time](#)
- [show log config](#)

log email time

Overview This command configures the time used in messages sent to an email address. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

Syntax `log email <email-address> time {local|local-offset|utc-offset {plus|minus}<0-24>}`

Parameter	Description
<email-address>	The email address to send log messages to
time	Specify the time difference between the email recipient and the device you are configuring.
local	The device is in the same time zone as the email recipient
local-offset	The device is in a different time zone to the email recipient. Use the plus or minus keywords and specify the difference (offset) from local time of the device to the email recipient in hours.
utc-offset	The device is in a different time zone to the email recipient. Use the plus or minus keywords and specify the difference (offset) from UTC time of the device to the email recipient in hours.
plus	Negative offset (difference) from the device to the email recipient.
minus	Positive offset (difference) from the device to the email recipient.
<0-24>	World Time zone offset in hours

Default The default is **local** time.

Mode Global Configuration

Usage notes Use the **local** option if the email recipient is in the same time zone as this device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the email recipient in hours. Messages will display the time they were generated on this device but converted to the time zone of the email recipient.

Examples To send messages to the email address `test@home.com` in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local 0
```

To send messages to the email address `admin@base.com` with the time information converted to the time zone of the email recipient, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local-offset plus
3
```

To send messages to the email address `user@remote.com` with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email user@remote.com time utc-offset minus
3
```

Related commands

- [default log email](#)
- [log email](#)
- [log email \(filter\)](#)
- [log email exclude](#)
- [show log config](#)

log facility

Overview Use this command to assign a facility to all log messages generated on this device. This facility overrides any facility that is automatically generated as part of the log message.

Use the **no** variant of this command to remove the configured facility.

Syntax `log facility {kern|user|mail|daemon|auth|syslog|lpr|news|uucp|cron|authpriv|ftp|local0|local1|local2|local3|local4|local5|local6|local7}`
`no log facility`

Default None. The outgoing syslog facility depends on the log message.

Mode Global Configuration

Usage notes Specifying different facilities for log messages generated on different devices can allow messages from multiple devices sent to a common server to be distinguished from each other.

Ordinarily, the facility values generated in log messages have meanings as shown in the following table. Using this command will override these meanings, and the new meanings will depend on the use you put them to.

Table 9-1: Ordinary meanings of the facility parameter in log messages

Facility	Description
kern	Kernel messages
user	User-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by the syslog daemon
lpr	Line printer subsystem
news	Network news subsystem
uucp	UNIX-to-UNIX Copy Program subsystem
cron	Clock daemon
authpriv	Security/authorization (private) messages

Table 9-1: Ordinary meanings of the facility parameter in log messages (cont.)

Facility	Description
ftp	FTP daemon
local<0..7>	The facility labels above have specific meanings, while the local facility labels are intended to be put to local use. In AlliedWare Plus, some of these local facility labels are used in log messages. In particular, local5 is assigned to log messages generated by UTM Firewall security features.

Example To specify a facility of local6, use the following commands:

```
awplus# configure terminal
awplus(config)# log facility local6
```

Related commands [show log config](#)

log host

Overview This command configures the device to send log messages to a remote syslog server via UDP port 514. The IP address of the remote server must be specified. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent.

Use the **no** variant of this command to stop sending log messages to the remote syslog server.

Syntax `log host <ipv4-addr> [secure]`
`log host <ipv6-addr>`
`no log host <ipv4-addr>|<ipv6-addr>`

Parameter	Description
<code><ipv4-addr></code>	Specify the source IPv4 address, in dotted decimal notation (A.B.C.D).
<code><ipv6-addr></code>	Specify the source IPv6 address, in X:X::X:X notation.
<code>secure</code>	Optional value to create a secure log destination. This option is only valid for IPv4 hosts.

Mode Global Configuration

Usage notes Use the optional **secure** parameter to configure a secure IPv4 syslog host. For secure hosts, syslog over TLS is used to encrypt the logs. The certificate received from the remote log server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

The remote server may also request that a certificate is transmitted from the local device. In this situation the first trustpoint added to the syslog application will be transmitted to the remote server.

For detailed information about securing syslog, see the [PKI Feature Overview_and Configuration_Guide](#).

Examples To configure the device to send log messages to a remote secure syslog server with IP address 10.32.16.99, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.99 secure
```

To stop the device from sending log messages to the remote syslog server with IP address 10.32.16.99, use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.99
```

Related commands [default log host](#)
[log host \(filter\)](#)

log host exclude
log host source
log host startup-delay
log host time
log trustpoint
show log config

**Command
changes**

Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log host (filter)

Overview This command creates a filter to select messages to be sent to a remote syslog server. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a substring within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a remote syslog server. The IP address of the syslog server must be specified. All configuration relating to this log target will be removed.

Syntax `log host <ip-addr> [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log host <ip-addr> [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]`

Parameter	Description																
<ip-addr>	The IP address of a remote syslog server.																
level	Filter messages by severity level.																
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: <table> <tr> <td>0 emergencies</td><td>System is unusable</td></tr> <tr> <td>1 alerts</td><td>Action must be taken immediately</td></tr> <tr> <td>2 critical</td><td>Critical conditions</td></tr> <tr> <td>3 errors</td><td>Error conditions</td></tr> <tr> <td>4 warnings</td><td>Warning conditions</td></tr> <tr> <td>5 notices</td><td>Normal, but significant, conditions</td></tr> <tr> <td>6 informational</td><td>Informational messages</td></tr> <tr> <td>7 debugging</td><td>Debug-level messages</td></tr> </table>	0 emergencies	System is unusable	1 alerts	Action must be taken immediately	2 critical	Critical conditions	3 errors	Error conditions	4 warnings	Warning conditions	5 notices	Normal, but significant, conditions	6 informational	Informational messages	7 debugging	Debug-level messages
0 emergencies	System is unusable																
1 alerts	Action must be taken immediately																
2 critical	Critical conditions																
3 errors	Error conditions																
4 warnings	Warning conditions																
5 notices	Normal, but significant, conditions																
6 informational	Informational messages																
7 debugging	Debug-level messages																
program	Filter messages by program. Include messages from a specified program.																
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. <table> <tr> <td>rip</td><td>Routing Information Protocol (RIP)</td></tr> <tr> <td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr> <tr> <td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr> <tr> <td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr> <tr> <td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr> <tr> <td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr> </table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)				
rip	Routing Information Protocol (RIP)																
ripng	Routing Information Protocol - next generation (RIPng)																
ospf	Open Shortest Path First (OSPF)																
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																
bgp	Border Gateway Protocol (BGP)																
rsvp	Resource Reservation Protocol (RSVP)																

Parameter	Description
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (DHCP SN)
facility	Filter messages by syslog facility.
<facility>	Specify one of the following syslog facilities to include messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Select messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Mode Global Configuration

Examples To create a filter to send all messages containing the text "Bridging initialization", to a remote syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 msgtext "Bridging
initialization"
```

To create a filter to send messages with a severity level of **informational** and above to the syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 level informational
```

To remove a filter that sends all messages containing the text "Bridging initialization", to a remote syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.21 msgtext "Bridging
initialization"
```

To remove a filter that sends messages with a severity level of **informational** and above to the syslog server with IP address 10.32.16.21, use the following commands:

```
awplusawpluls# configure terminal
awplus(config)# no log host 10.32.16.21 level informational
```

Related commands

- [default log host](#)
- [log host](#)
- [log host exclude](#)
- [log host source](#)
- [log host time](#)
- [show log config](#)

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log host exclude

Overview Use this command to prevent specified log messages from being sent to the remote syslog server, when **log host** is enabled. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax `log host {<hostname>|<ipv4-addr>|<ipv6-addr>} exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`
`no log host {<hostname>|<ipv4-addr>|<ipv6-addr>} exclude [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

Parameter	Description																
<hostname>	The host name of a remote syslog server.																
<ipv4-addr>	The IPv4 address of a remote syslog server, in A.B.C.D format.																
<ipv6-addr>	The IPv6 address of a remote syslog server, in X:X::X:X format.																
level	Exclude messages of the specified severity level.																
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: <table><tr><td>0 emergencies</td><td>System is unusable</td></tr><tr><td>1 alerts</td><td>Action must be taken immediately</td></tr><tr><td>2 critical</td><td>Critical conditions</td></tr><tr><td>3 errors</td><td>Error conditions</td></tr><tr><td>4 warnings</td><td>Warning conditions</td></tr><tr><td>5 notices</td><td>Normal, but significant, conditions</td></tr><tr><td>6 informational</td><td>Informational messages</td></tr><tr><td>7 debugging</td><td>Debug-level messages</td></tr></table>	0 emergencies	System is unusable	1 alerts	Action must be taken immediately	2 critical	Critical conditions	3 errors	Error conditions	4 warnings	Warning conditions	5 notices	Normal, but significant, conditions	6 informational	Informational messages	7 debugging	Debug-level messages
0 emergencies	System is unusable																
1 alerts	Action must be taken immediately																
2 critical	Critical conditions																
3 errors	Error conditions																
4 warnings	Warning conditions																
5 notices	Normal, but significant, conditions																
6 informational	Informational messages																
7 debugging	Debug-level messages																
program	Exclude messages from a specified program.																
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.																

Parameter	Description
rip	Routing Information Protocol (RIP)
ripng	Routing Information Protocol - next generation (RIPng)
ospf	Open Shortest Path First (OSPF)
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)
bgp	Border Gateway Protocol (BGP)
rsvp	Resource Reservation Protocol (RSVP)
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (DHCP SN)
facility	Exclude messages from a syslog facility.
<facility>	Specify one of the following syslog facilities to exclude messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon

Parameter	Description
	authpriv Security/authorization messages (private)
	ftp FTP daemon
msgtext	Exclude messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default No log messages are excluded

Mode Global configuration

Example To exclude messages that contain the string 'example of irrelevant message' being sent to the remote syslog server 10.10.10.100, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.10.10.100 exclude msgtext example
of irrelevant message
```

Related commands

- [default log host](#)
- [log host](#)
- [log host \(filter\)](#)
- [log host source](#)
- [log host time](#)
- [show log config](#)

Command changes Version 5.2.2-1.1: **vrf** parameter added for products that support VRF

log host source

Overview Use this command to specify a source interface or IP address for the device to send syslog messages from. You can specify any one of an interface name, an IPv4 address or an IPv6 address.

This is useful if the device can reach the syslog server via multiple interfaces or addresses and you want to control which interface/address the device uses.

Note that AlliedWare Plus does not support source interface settings on secure log hosts (which are hosts configured using “log host <ip-address> secure”).

Use the **no** variant of this command to stop specifying a source interface or address.

Syntax `log host source {<interface-name>|<ipv4-addr>|<ipv6-addr>}`
`no log host source`

Parameter	Description
<interface-name>	Specify the source interface name. You can enter an Eth interface or loopback interface.
<ipv4-addr>	Specify the source IPv4 address, in dotted decimal notation (A.B.C.D).
<ipv6-addr>	Specify the source IPv6 address, in X:X::X:X notation.

Default None (no source is configured)

Mode Global Configuration

Example To send syslog messages from 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# log host source 192.168.1.1
```

Related commands

- [default log host](#)
- [log host](#)
- [log host \(filter\)](#)
- [log host exclude](#)
- [log host time](#)
- [show log config](#)

log host startup-delay

Overview Use this command to set the delay between the device booting up and it attempting to connect to remote log hosts. This is to allow time for network connectivity to the remote host to be established. During this period, the device buffers log messages and sends them once it has connected to the remote host.

The startup delay begins when the message "syslog-ng starting up" appears in the log.

If the default startup delay is not long enough for the boot and configuration process to complete and the links to come up, you may see logging failure messages on startup. In these cases, you can use the command to increase the startup delay.

Use the **no** variant of this command to return to the default delay values.

Syntax `log host startup-delay [delay <1-600>] [messages <1-5000>]`
`no log host startup-delay`

Parameter	Description
<code>delay <1-600></code>	The time, in seconds, from when syslog starts before the device attempts to filter and transmit the buffered messages to remote hosts.
<code>messages <1-5000></code>	The maximum number of messages that the device will buffer during the delay period.

Default By default the system will buffer up to 2000 messages and wait 120 seconds from when syslog starts before attempting to filter and transmit the buffered messages to remote hosts.

Mode Global Configuration

Example To increase the delay to 180 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# log host startup-delay delay 180
```

Related commands

- [default log host](#)
- [log host \(filter\)](#)
- [log host exclude](#)
- [log host source](#)
- [log host time](#)
- [log trustpoint](#)
- [show log config](#)

Command changes Version 5.4.8-0.2: defaults changed

log host time

Overview This command configures the time used in messages sent to a remote syslog server. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

Syntax `log host {<hostname>|<ipv4-addr>|<ipv6-addr>} time {local|local-offset|utc-offset {plus|minus} <0-24>}`

Parameter	Description
<hostname>	The host name of a remote syslog server.
<ipv4-addr>	The IPv4 address of a remote syslog server, in A.B.C.D format.
<ipv6-addr>	The IPv6 address of a remote syslog server, in X:X::X:X format.
<email-address>	The email address to send log messages to
time	Specify the time difference between the email recipient and the device you are configuring.
local	The device is in the same time zone as the email recipient
local-offset	The device is in a different time zone to the email recipient. Use the plus or minus keywords and specify the difference (offset) from local time of the device to the email recipient in hours.
utc-offset	The device is in a different time zone to the email recipient. Use the plus or minus keywords and specify the difference (offset) from UTC time of the device to the email recipient in hours.
plus	Negative offset (difference) from the device to the syslog server.
minus	Positive offset (difference) from the device to the syslog server.
<0-24>	World Time zone offset in hours

Default The default is **local** time.

Mode Global Configuration

Usage notes Use the **local** option if the remote syslog server is in the same time zone as the device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the remote syslog server in hours. Messages will display the time they were generated on this device but converted to the time zone of the remote syslog server.

Examples To send messages to the remote syslog server with the IP address 10.32.16.21 in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 time local 0
```

To send messages to the remote syslog server with the IP address 10.32.16.12 with the time information converted to the time zone of the remote syslog server, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.12 time local-offset plus 3
```

To send messages to the remote syslog server with the IP address 10.32.16.02 with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.02 time utc-offset minus 3
```

Related commands

- [default log host](#)
- [log host](#)
- [log host \(filter\)](#)
- [log host exclude](#)
- [log host source](#)
- [show log config](#)

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log monitor (filter)

Overview This command creates a filter to select messages to be sent to the terminal when the **terminal monitor** command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

Syntax `log monitor [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`
`no log monitor [level <level>] [program <program-name>] [facility <facility>] [msgtext <text-string>]`

Parameter	Description																		
level	Filter messages by severity level.																		
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity: <table><tr><td>0 emergencies</td><td>System is unusable</td></tr><tr><td>1 alerts</td><td>Action must be taken immediately</td></tr><tr><td>2 critical</td><td>Critical conditions</td></tr><tr><td>3 errors</td><td>Error conditions</td></tr><tr><td>4 warnings</td><td>Warning conditions</td></tr><tr><td>5 notices</td><td>Normal, but significant, conditions</td></tr><tr><td>6 informational</td><td>Informational messages</td></tr><tr><td>7 debugging</td><td>Debug-level messages</td></tr></table>	0 emergencies	System is unusable	1 alerts	Action must be taken immediately	2 critical	Critical conditions	3 errors	Error conditions	4 warnings	Warning conditions	5 notices	Normal, but significant, conditions	6 informational	Informational messages	7 debugging	Debug-level messages		
0 emergencies	System is unusable																		
1 alerts	Action must be taken immediately																		
2 critical	Critical conditions																		
3 errors	Error conditions																		
4 warnings	Warning conditions																		
5 notices	Normal, but significant, conditions																		
6 informational	Informational messages																		
7 debugging	Debug-level messages																		
program	Filter messages by program. Include messages from a specified program.																		
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are. <table><tr><td>rip</td><td>Routing Information Protocol (RIP)</td></tr><tr><td>ripng</td><td>Routing Information Protocol - next generation (RIPng)</td></tr><tr><td>ospf</td><td>Open Shortest Path First (OSPF)</td></tr><tr><td>ospfv3</td><td>Open Shortest Path First (OSPF) version 3 (OSPFv3)</td></tr><tr><td>bgp</td><td>Border Gateway Protocol (BGP)</td></tr><tr><td>rsvp</td><td>Resource Reservation Protocol (RSVP)</td></tr><tr><td>pim-dm</td><td>Protocol Independent Multicast - Dense Mode (PIM-DM)</td></tr><tr><td>pim-sm</td><td>Protocol Independent Multicast - Sparse Mode (PIM-SM)</td></tr><tr><td>pim-smv6</td><td>PIM-SM version 6 (PIM-SMv6)</td></tr></table>	rip	Routing Information Protocol (RIP)	ripng	Routing Information Protocol - next generation (RIPng)	ospf	Open Shortest Path First (OSPF)	ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)	bgp	Border Gateway Protocol (BGP)	rsvp	Resource Reservation Protocol (RSVP)	pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)	pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)	pim-smv6	PIM-SM version 6 (PIM-SMv6)
rip	Routing Information Protocol (RIP)																		
ripng	Routing Information Protocol - next generation (RIPng)																		
ospf	Open Shortest Path First (OSPF)																		
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)																		
bgp	Border Gateway Protocol (BGP)																		
rsvp	Resource Reservation Protocol (RSVP)																		
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)																		
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)																		
pim-smv6	PIM-SM version 6 (PIM-SMv6)																		

Parameter	Description
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpcsn	DHCP snooping (DHPCPSN)
facility	Filter messages by syslog facility.
<facility>	Specify one of the following syslog facilities to include messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Select messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default By default there is a filter to select all messages. This filter may be removed and replaced by filters that are more selective.

Mode Global Configuration

Examples To create a filter to send all messages that are generated by authentication and have a severity of **info** or higher to terminal instances where the terminal monitor command has been given, use the following commands:

```
awplus# configure terminal
awplus(config)# log monitor level info program auth
```

To remove a default filter that includes sending everything to the terminal, use the following commands:

```
awplus# configure terminal
awplus(config)# no log monitor level debugging
```

Related commands

- [default log monitor](#)
- [log monitor exclude](#)
- [show log config](#)
- [terminal monitor](#)

log monitor exclude

Overview Use this command to prevent specified log messages from being displayed on a terminal, when **terminal monitor** is enabled. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax `log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]`

Parameter	Description
level	Exclude messages of the specified severity level.
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:
0 emergencies	System is unusable
1 alerts	Action must be taken immediately
2 critical	Critical conditions
3 errors	Error conditions
4 warnings	Warning conditions
5 notices	Normal, but significant, conditions
6 informational	Informational messages
7 debugging	Debug-level messages
program	Exclude messages from a specified program.
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.
rip	Routing Information Protocol (RIP)
ripng	Routing Information Protocol - next generation (RIPng)
ospf	Open Shortest Path First (OSPF)
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)

Parameter	Description
bgp	Border Gateway Protocol (BGP)
rsvp	Resource Reservation Protocol (RSVP)
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpsn	DHCP snooping (DHCP SN)
facility	Exclude messages from a syslog facility.
<facility>	Specify one of the following syslog facilities to exclude messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon

Parameter	Description
msgtext	Exclude messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log monitor exclude msgtext example of
irrelevant message
```

Related commands

- [default log monitor](#)
- [log monitor \(filter\)](#)
- [show log config](#)
- [terminal monitor](#)

log permanent

Overview This command configures the device to send permanent log messages to non-volatile storage (NVS) on the device. The content of the permanent log is retained over a reboot. Once the permanent log reaches its configured maximum allowable size old messages will be deleted to make way for new messages.

The **no** variant of this command configures the device not to send any messages to the permanent log. Log messages will not be retained over a restart.

Syntax `log permanent`
`no log permanent`

Mode Global Configuration

Examples To enable permanent logging use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent
```

To disable permanent logging use the following commands:

```
awplus# configure terminal
awplus(config)# no log permanent
```

Related commands

- `clear log permanent`
- `copy permanent-log`
- `default log permanent`
- `log permanent (filter)`
- `log permanent exclude`
- `log permanent size`
- `show log config`
- `show log permanent`

log permanent (filter)

Overview This command creates a filter to select messages to be sent to the permanent log. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the permanent log.

Syntax `log permanent [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log permanent [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]`

Parameter	Description
level	Filter messages sent to the permanent log by severity level.
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:
0 emergencies	System is unusable
1 alerts	Action must be taken immediately
2 critical	Critical conditions
3 errors	Error conditions
4 warnings	Warning conditions
5 notices	Normal, but significant, conditions
6 informational	Informational messages
7 debugging	Debug-level messages
program	Filter messages by program. Include messages from a specified program.
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.
rip	Routing Information Protocol (RIP)
ripng	Routing Information Protocol - next generation (RIPng)
ospf	Open Shortest Path First (OSPF)
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)
bgp	Border Gateway Protocol (BGP)
rsvp	Resource Reservation Protocol (RSVP)
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)

Parameter	Description
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpcsn	DHCP snooping (DHCP SN)
facility	Filter messages by syslog facility.
<facility>	Specify one of the following syslog facilities to include messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Select messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default By default the buffered log has a filter to select messages whose severity level is `notices` (5) or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To create a filter to send all messages containing the text “Bridging initialization”, to the permanent log use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent msgtext Bridging initialization
```

Related commands

- clear log permanent
- default log permanent
- log permanent
- log permanent exclude
- log permanent size
- show log config
- show log permanent

log permanent exclude

Overview Use this command to prevent specified log messages from being sent to the permanent log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax `log permanent exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
no log permanent exclude [level <level>] [program
<program-name>] [facility <facility>] [msgtext <text-string>]`

Parameter	Description
level	Exclude messages of the specified severity level.
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:
0 emergencies	System is unusable
1 alerts	Action must be taken immediately
2 critical	Critical conditions
3 errors	Error conditions
4 warnings	Warning conditions
5 notices	Normal, but significant, conditions
6 informational	Informational messages
7 debugging	Debug-level messages
program	Exclude messages from a specified program.
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.
rip	Routing Information Protocol (RIP)
ripng	Routing Information Protocol - next generation (RIPng)
ospf	Open Shortest Path First (OSPF)
ospfv3	Open Shortest Path First (OSPF) version 3 (OSPFv3)
bgp	Border Gateway Protocol (BGP)

Parameter	Description
rsvp	Resource Reservation Protocol (RSVP)
pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
pim-smv6	PIM-SM version 6 (PIM-SMv6)
dot1x	IEEE 802.1X Port-Based Access Control
lacp	Link Aggregation Control Protocol (LACP)
stp	Spanning Tree Protocol (STP)
rstp	Rapid Spanning Tree Protocol (RSTP)
mstp	Multiple Spanning Tree Protocol (MSTP)
imi	Integrated Management Interface (IMI)
imish	Integrated Management Interface Shell (IMISH)
epsr	Ethernet Protection Switched Rings (EPSR)
irdp	ICMP Router Discovery Protocol (IRDP)
rmon	Remote Monitoring
loopprot	Loop Protection
poe	Power-inline (Power over Ethernet)
dhcpcsn	DHCP snooping (DHPCPSN)
facility	Exclude messages from a syslog facility.
<facility>	Specify one of the following syslog facilities to exclude messages from:
kern	Kernel messages
user	Random user-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by syslogd
lpr	Line printer subsystem
news	Network news subsystem
uucp	UUCP subsystem
cron	Clock daemon
authpriv	Security/authorization messages (private)
ftp	FTP daemon
msgtext	Exclude messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent exclude msgtext example of
irrelevant message
```

Related commands

- [clear log permanent](#)
- [default log permanent](#)
- [log permanent](#)
- [log permanent \(filter\)](#)
- [log permanent size](#)
- [show log config](#)
- [show log permanent](#)

log permanent size

Overview This command configures the amount of memory that the permanent log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

Use the **no** variant of this command to return to the default.

Syntax `log permanent size <50-250>`
`no log permanent size`

Parameter	Description
<50-250>	Size of the permanent log in kilobytes

Default 50 kilobytes

Mode Global Configuration

Example To allow the permanent log to use up to 100 kilobytes of NVS, use the commands:

```
awplus# configure terminal
awplus(config)# log permanent size 100
```

To return to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no log permanent size
```

Related commands

- [clear log permanent](#)
- [copy permanent-log](#)
- [default log permanent](#)
- [log permanent](#)
- [log permanent \(filter\)](#)
- [log permanent exclude](#)
- [show log config](#)
- [show log permanent](#)

log-rate-limit nsm

Overview This command limits the number of log messages generated by the device for a specified time interval.

Use the **no** variant of this command to revert to the default number of log messages, which is up to 200 log messages per second.

Syntax `log-rate-limit nsm messages <message-limit> interval
<time-interval>`
`no log-rate-limit nsm`

Parameter	Description
<code><message-limit></code>	<code><1-65535></code> The number of log messages generated by the device.
<code><time-interval></code>	<code><0-65535></code> The time period for log message generation in 1/100 seconds. If an interval of 0 is specified then no log message rate limiting is applied.

Default By default, the device will allow 200 log messages to be generated per second.

Mode Global Configuration

Usage notes This command limits the rate that log messages are generated. Limiting log messages protects the device from running out of memory in extreme conditions, such as during a broadcast storm.

Once the specified number of log messages per interval is exceeded, any excess log messages are dropped. When this occurs a summary log message is generated at the end of the interval. This summary message includes the number of log messages dropped.

If you expect a lot of dropped log messages, we recommend setting the time interval to no less than 100. This limits the number of summary messages to one per second, which prevents the log from filling up with these summary messages.

Examples To allow the device to generate a maximum of 300 log messages per second, use the following commands:

```
awplus# configure terminal
awplus(config)# log-rate-limit nsm messages 300 interval 100
```

To return the device to the default setting, use the following commands:

```
awplus# configure terminal
awplus(config)# no log-rate-limit nsm
```

log trustpoint

Overview This command adds one or more trustpoints to be used with the syslog application. Multiple trustpoints may be specified, or the command may be executed multiple times, to add multiple trustpoints to the application.

The **no** version of this command removes one or more trustpoints from the list of trustpoints associated with the application.

Syntax `log trustpoint [<trustpoint-list>]`
`no log trustpoint [<trustpoint-list>]`

Parameter	Description
<trustpoint-list>	Specify one or more trustpoints to be added or deleted.

Default No trustpoints are created by default.

Mode Global Configuration

Usage notes The device certificate associated with first trustpoint added to the application will be transmitted to remote servers. The certificate received from the remote server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

If no trustpoints are specified in the command, the trustpoint list will be unchanged.

If **no log trustpoint** is issued without specifying any trustpoints, then all trustpoints will be disassociated from the application.

Example You can add multiple trustpoints by executing the command multiple times:

```
awplus# configure terminal
awplus(config)# log trustpoint trustpoint_1
awplus(config)# log trustpoint trustpoint_2
```

Alternatively, add multiple trustpoints with a single command:

```
awplus(config)# log trustpoint trustpoint_2 trustpoint_3
```

Disassociate all trustpoints from the syslog application using the command:

```
awplus(config)# log trustpoint trustpoint_2 trustpoint_3
```

Related commands [log host](#)
[show log config](#)

log url-requests

Overview If URL Filtering is enabled, then by default, black list hits and issues with match criteria and list files are logged.

Use this command to enable logging of all HTTP and HTTPS URL requests (both permitted and denied) passing through the firewall.

Use the **no** variant of this command to disable extra logging of HTTP and HTTPS URL requests passing through the firewall.

Syntax `log url-requests`
`no log url-requests`

Default Disabled by default.

Mode URL Filter Configuration

Usage notes When enabled, additional log messages for HTTP and HTTPS URL requests passing through the firewall contain the:

- URL being accessed
- IP address of the user that requested the URL

Example To configure logging of all HTTP and HTTPS URL requests passing through the firewall (permitted as well as denied), use the following commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# log url-requests
```

Related commands [url-filter](#)

Command changes Version 5.4.7-1.1: command added

show connection-log events

Overview This command displays the configuration state (enabled or disabled) for the logging of connections passing through the firewall, as configured by the [connection-log events](#) command.

Syntax `show connection-log events`

Mode User Exec

Example To show the logging configuration state for the connections passing through the firewall, use the command:

```
awplus# show connection-log events
```

Output Figure 9-1: Example output from **show connection-log events**

```
awplus#show connection-log events
Log new connection events:      Disabled
Log connection end events:     Enabled
```

Related commands [connection-log events](#)

Command changes Version 5.4.7-1.1: command added.

show counter log

Overview This command displays log counter information.

Syntax `show counter log`

Mode User Exec and Privileged Exec

Example To display the log counter information, use the command:

```
awplus# show counter log
```

Output Figure 9-2: Example output from the **show counter log** command

Log counters	
Total Received	 2328
Total Received P0	 0
Total Received P1	 0
Total Received P2	 1
Total Received P3	 9
Total Received P4	 32
Total Received P5	 312
Total Received P6	 1602
Total Received P7	 372

Table 10: Parameters in output of the **show counter log** command

Parameter	Description
Total Received	Total number of messages received by the log
Total Received P0	Total number of Priority 0 (Emergency) messages received
Total Received P1	Total number of Priority 1 (Alert) messages received
Total Received P2	Total number of Priority 2 (Critical) messages received
Total Received P3	Total number of Priority 3 (Error) messages received
Total Received P4	Total number of Priority 4 (Warning) messages received
Total Received P5	Total number of Priority 5 (Notice) messages received
Total Received P6	Total number of Priority 6 (Info) messages received
Total Received P7	Total number of Priority 7 (Debug) messages received

Related commands [show log config](#)

show exception log

Overview This command displays the contents of the exception log. If the device has unexpectedly restarted and has produced a core dump file, the output of this command shows the name and location of the file.

Syntax `show exception log`

Mode User Exec and Privileged Exec

Example To display the exception log, use the command:

```
awplus# show exception log
```

Output Figure 9-3: Example output from the **show exception log** command on a device that has never had an exception occur

```
awplus#show exception log
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-----
None
-----
awplus#
```

show log

Overview This command displays the contents of the buffered log.
For information on filtering and saving command output, see the [“Getting Started with AlliedWare_Plus” Feature Overview and Configuration Guide](#).

Syntax `show log [tail [<10-250>]]`

Parameter	Description
tail	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Default By default the entire contents of the buffered log is displayed.

Mode User Exec, Privileged Exec and Global Configuration

Usage notes If the optional **tail** parameter is specified, only the latest 10 messages in the buffered log are displayed. A numerical value can be specified after the **tail** parameter to select how many of the latest messages should be displayed.
The **show log** command is only available to users at privilege level 7 and above. To set a user’s privilege level, use the command:

```
awplus(config)# username <name> privilege <1-15>
```

Examples To display the contents of the buffered log use the command:

```
awplus# show log
```

To display the 10 latest entries in the buffered log use the command:

```
awplus# show log tail 10
```

Output Figure 9-4: Example output from **show log**

```
awplus#show log

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-----
2023 Feb 11 00:38:04 syslog.notice awplus syslog-ng[150]: syslog-ng starting up;
version='3.21.1'
2023 Feb 11 00:38:05 syslog.notice awplus syslog-ng[150]: Configuration reload
request received, reloading configuration;
2023 Feb 11 00:38:07 syslog.notice awplus syslog-ng[150]: Configuration reload
finished;
2023 Feb 11 00:38:07 user.notice awplus IMI[689]: no clock timezone: previous
time 00:38:07 11 Feb 2023, new time 00:38:07 11 Feb 2023
2023 Feb 11 00:38:08 user.notice awplus IMI[689]: AlliedWare Plus(TM) v5.5.3_0
startup at 00:38:08 11 Feb 2023.
2023 Feb 11 00:38:08 user.notice awplus IMISH[1200]: [SCRIPT]privilege 1
2023 Feb 11 00:38:08 user.notice awplus IMISH[1200]: [SCRIPT]exec-timeout 10 0
2023 Feb 11 00:38:08 user.notice awplus IMISH[1200]: [SCRIPT]no length
...
```

Related commands

- [clear log buffered](#)
- [copy buffered-log](#)
- [default log buffered](#)
- [log buffered](#)
- [log buffered \(filter\)](#)
- [log buffered size](#)
- [log buffered exclude](#)
- [show log config](#)

show log config

Overview This command displays information about the logging system. This includes the configuration of the various log destinations, such as buffered, permanent, syslog servers (hosts) and email addresses. This also displays the latest status information for each log destination.

Syntax show log config

Mode User Exec, Privileged Exec and Global Configuration

Example To display the logging configuration use the command:

```
awplus# show log config
```

Output Figure 9-5: Example output from **show log config**

```
Facility: default

PKI trustpoints: example_trustpoint

Buffered log:
Status ..... enabled
Maximum size ... 100kb
Filters:
*1 Level ..... notices
  Program ..... any
  Facility ..... any
  Message text . any
  2 Level ..... informational
    Program ..... auth
    Facility ..... daemon
    Message text . any
  Statistics ..... 1327 messages received, 821 accepted by filter (2016 Oct 11
10:36:16)
Permanent log:
Status ..... enabled
Maximum size ... 60kb
Filters:
  1 Level ..... error
    Program ..... any
    Facility ..... any
    Message text . any
  *2 Level ..... warnings
    Program ..... dhcp
    Facility ..... any
    Message text . "pool exhausted"
  Statistics ..... 1327 messages received, 12 accepted by filter (2016 Oct 11
10:36:16)
```

```
Host 10.32.16.21:
  Time offset .... +2:00
  Offset type .... UTC
  Source ..... -
  Secured ..... enabled
  Filters:
  1 Level ..... critical
    Program ..... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 1 accepted by filter (2016 Oct 11
10:36:16)
Email admin@alliedtelesis.com:
  Time offset .... +0:00
  Offset type .... Local
  Filters:
  1 Level ..... emergencies
    Program ..... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 0 accepted by filter (2016 Oct 11
10:36:16)
...
```

In the above example the '*' next to filter 1 in the buffered log configuration indicates that this is the default filter. The permanent log has had its default filter removed, so none of the filters are marked with '*'.

NOTE: Terminal log and console log cannot be set at the same time. If console logging is enabled then the terminal logging is turned off.

Related commands

- [show counter log](#)
- [show log](#)
- [show log permanent](#)

show log permanent

Overview This command displays the contents of the permanent log.

Syntax `show log permanent [tail [<10-250>]]`

Parameter	Description
tail	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Usage notes If the optional **tail** parameter is specified, only the latest 10 messages in the permanent log are displayed. A numerical value can be specified after the **tail** parameter to change how many of the latest messages should be displayed.

Mode User Exec, Privileged Exec and Global Configuration

Example To display the permanent log, use the command:

```
awplus# show log permanent
```

Output Figure 9-6: Example output from **show log permanent**

```
awplus> show log permanent

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
-----
2025-04-22T14:17:01+12:00 daemon.err NZTA-VFW radiusd[484]: Ignoring request to auth
address * port 1901 bound to server default from unknown client 172.31.5.30 port
4272 proto udp
2025-04-22T14:17:06+12:00 daemon.err NZTA-VFW radiusd[484]: Ignoring request to auth
address * port 1901 bound to server default from unknown client 172.31.5.30 port
4270 proto udp
2025-04-22T14:17:07+12:00 daemon.err NZTA-VFW radiusd[484]: Ignoring request to auth
address * port 1901 bound to server default from unknown client 172.31.5.30 port
4271 proto udp
2025-04-22T14:17:08+12:00 daemon.err NZTA-VFW radiusd[484]: Ignoring request to auth
address * port 1901 bound to server default from unknown client 172.31.5.30 port
4272 proto udp
...
```

Related commands

- [clear log permanent](#)
- [copy permanent-log](#)
- [default log permanent](#)
- [log permanent](#)
- [log permanent \(filter\)](#)
- [log permanent exclude](#)

log permanent size

show log config

show running-config log

Overview This command displays the current running configuration of the Log utility.

Syntax `show running-config log`

Mode Privileged Exec and Global Configuration

Example To display the current configuration of the log utility, use the command:

```
awplus# show running-config log
```

Related commands [show log](#)
[show log config](#)

10

Scripting Commands

Introduction

Overview This chapter provides commands used for command scripts.

- Command List**
- `activate` on page 374
 - `echo` on page 375
 - `wait` on page 376

activate

Overview This command activates a script file.

Syntax `activate [background] <script>`

Parameter	Description
<code>background</code>	Activate a script to run in the background. A process that is running in the background will operate as a separate task, and will not interrupt foreground processing. Generally, we recommend running short, interactive scripts in the foreground and longer scripts in the background. The default is to run the script in the foreground.
<code><script></code>	The file name of the script to activate. The script is a command script consisting of commands documented in this software reference. Note that you must use either a .scp or a .sh filename extension for a valid script text file, as described below in the usage section for this command.

Mode Privileged Exec

Usage notes When a script is activated, the privilege level is set to 1 enabling User Exec commands to run in the script. If you need to run Privileged Exec commands in your script you need to add an [enable \(Privileged Exec mode\)](#) command to the start of your script. If you need to run Global Configuration commands in your script you need to add a [configure terminal](#) command after the **enable** command at the start of your script.

The **activate** command executes the script in a new shell. A [terminal length](#) shell command, such as **terminal length 0** may also be required to disable a delay that would pause the display.

A script must be a text file with a filename extension of either **.sh** or **.scp** only for the AlliedWare Plus CLI to activate the script file. The **.sh** filename extension indicates the file is an ASH script, and the **.scp** filename extension indicates the file is an AlliedWare Plus script.

Examples To activate a command script to run as a background process, use the command:

```
awplus#activate background test.scp
```

Related commands

- [configure terminal](#)
- [echo](#)
- [enable \(Privileged Exec mode\)](#)
- [wait](#)

echo

Overview This command echoes a string to the terminal, followed by a blank line.

Syntax `echo <line>`

Parameter	Description
<code><line></code>	The string to echo

Mode User Exec and Privileged Exec

Usage This command may be useful in CLI scripts, to make the script print user-visible comments.

Example To echo the string `Hello World` to the console, use the command:
`awplus# echo Hello World`

Output

```
Hello World
```

Related commands [activate](#)
[wait](#)

wait

Overview This command pauses execution of the active script for the specified period of time.

Syntax `wait <delay>`

Parameter	Description
<code><delay></code>	<code><1-65535></code> Specify the time delay in seconds

Default No wait delay is specified by default.

Mode Privileged Exec (when executed from a script not directly from the command line)

Usage notes Use this command to pause script execution in an **.scp** (AlliedWare Plus™ script) or an **.sh** (ASH script) file executed by the [activate](#) command. The script must contain an **enable** command, because the **wait** command is only executed in the Privileged Exec mode.

Example See an **.scp** script file extract below that will show port counters for interface eth0 over a 10 second interval:

```
enable

show interface eth0

wait 10

show interface eth0
```

Related commands [activate](#)
[echo](#)
[enable \(Privileged Exec mode\)](#)

11

Interface Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure and display interfaces.

- Command List**
- “[description \(interface\)](#)” on page 378
 - “[interface \(to configure\)](#)” on page 379
 - “[ip tcp adjust-mss](#)” on page 381
 - “[ipv6 tcp adjust-mss](#)” on page 383
 - “[mtu](#)” on page 385
 - “[service statistics interfaces counter](#)” on page 387
 - “[show interface](#)” on page 388
 - “[show interface brief](#)” on page 391
 - “[show interface status](#)” on page 392
 - “[shutdown](#)” on page 394

description (interface)

Overview Use this command to add a description to a specific port or interface.

Syntax `description <description>`

Parameter	Description
<code><description></code>	Text describing the specific interface. Descriptions can contain any printable ASCII characters (ASCII 32-126).

Mode Interface Configuration

Example The following example uses this command to describe the device that an interface is connected to.

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# description Master Link
```

Command changes Version 5.4.7-1.1: valid character set changed to printable ASCII characters

interface (to configure)

Overview Use this command to select one or more interfaces to configure.

Syntax `interface <interface-list>`

Parameter	Description
<code><interface-list></code>	The interfaces to configure. An interface-list can be: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. The specified interfaces must exist.

Usage notes A local loopback interface is one that is always available for higher layer protocols to use and advertise to the network. Although a local loopback interface is assigned an IP address, it does not have the usual requirement of connecting to a lower layer physical entity. This lack of physical attachment creates the perception of a local loopback interface always being accessible via the network.

Local loopback interfaces can be utilized by a number of protocols for various purposes. They can be used to improve access to the device and also increase its reliability, security, scalability and protection. In addition, local loopback interfaces can add flexibility and simplify management, information gathering and filtering.

One example of this increased reliability is for OSPF to advertise a local loopback interface as an interface-route into the network irrespective of the physical links that may be 'up' or 'down' at the time. This provides a higher probability that the routing traffic will be received and subsequently forwarded.

Mode Global Configuration

Examples The following example shows how to enter Interface mode to configure the Ethernet interface eth0.2. Note how the prompt changes.

```
awplus# configure terminal
awplus(config)# interface eth0.2
awplus(config-if)#
```

The following example shows how to enter Interface mode to configure the PPP interface ppp0.

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)#
```

The following example shows how to enter Interface mode to configure the local loopback interface.

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)#
```

The following example shows how to enter Interface mode to configure bridge br2.

```
awplus# configure terminal
awplus(config)# interface br2
awplus(config-if)#
```

**Related
commands**

[ip address \(IP Addressing and Protocol\)](#)

[show interface](#)

[show interface brief](#)

ip tcp adjust-mss

Overview Use this command to set the Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

Syntax `ip tcp adjust-mss {<mss-size>|pmtu}`
`no ip tcp adjust-mss`

Parameter	Description
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	Adjust TCP MSS automatically with respect to the MTU on the interface.

Default The default setting allows a TCP server or a TCP client to set the MSS value for itself.

Mode Interface Configuration

Usage notes When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel

Examples To configure an MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ip tcp adjust-mss 1452
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip tcp adjust-mss
```

**Related
commands**

[mtu \(PPP\)](#)
[show interface](#)
[show interface \(PPP\)](#)

**Command
changes**

Version 5.4.8-2.1: interface tunnel example added

ipv6 tcp adjust-mss

Overview Use this command to set the IPv6 Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

Syntax `ipv6 tcp adjust-mss {<mss-size>|pmtu}`
`no ipv6 tcp adjust-mss`

Parameter	Description
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	Adjust TCP MSS automatically with respect to the MTU on the interface.

Default The default setting allows a TCP server or a TCP client to set the MSS value for itself.

Mode Interface Configuration

Usage notes When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel

Examples To configure an IPv6 MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To configure an IPv6 MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To adjust IPv6 TCP MSS automatically with respect to the MTU on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ipv6 tcp adjust-mss pmtu
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 tcp adjust-mss
```

**Related
commands**

[mtu \(PPP\)](#)
[show interface](#)
[show interface \(PPP\)](#)
[show interface tunnel \(GRE\)](#)

**Command
changes**

Version 5.4.8-2.1: interface tunnel example added

mtu

Overview Use this command to set the Maximum Transmission Unit (MTU) size for interfaces, where MTU is the maximum packet size that interfaces can transmit. The MTU size setting is applied to both IPv4 and IPv6 packet transmission.

Use the **no** variant of this command to remove a previously specified Maximum Transmission Unit (MTU) size, and restore the default MTU size. For example, the eth interface default is 1500 bytes.

Syntax `mtu <68-1582>`
`no mtu`

Parameter	Description
<code><68-1582></code>	The Maximum Transmission size in bytes.

Default The default MTU size, for example 1500 bytes for eth interfaces.

Mode Interface Configuration

Usage notes If a device receives an IPv4 packet for Layer 3 switching to another interface with an MTU size smaller than the packet size, and if the packet has the '**don't fragment**' bit set, then the device will send an ICMP '**destination unreachable**' (3) packet type and a '**fragmentation needed and DF set**' (4) code back to the source. For IPv6 packets bigger than the MTU size of the transmitting interface, an ICMP '**packet too big**' (ICMP type 2 code 0) message is sent to the source.

You can set a feasible MTU value on the following interfaces:

- PPP
- Ethernet
- Tunnel

Note that you cannot configure MTU on bridge interfaces. The MTU of the bridge interface is determined by the member interface of the bridge which has the lowest MTU. For example, if you attach eth0 with MTU 1200 and tunnel1 with MTU 1500 to a bridge interface, the MTU for that interface will be 1200.

Examples To configure an MTU size of 1555 bytes for tunnel 'tunnel2', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# mtu 1555
```

Related commands [show interface](#)

- Command changes**
- Version 5.4.7-1.1: Behavior change when MTU set to less than 1500 on FS980M and GS980M.
 - Version 5.5.1-0.1: Layer 3 jumbo frames supported on SBx908 GEN2 and x950.
 - Version 5.5.1-1.2: Layer 3 jumbo frames supported on x530 and GS980MX.

service statistics interfaces counter

Overview Use this command to enable the interface statistics counter.
Use the **no** variant of this command to disable the interface statistics counter.

Syntax `service statistics interfaces counter`
`no service statistics interfaces counter`

Default The interface statistics counter is enabled by default.

Mode Global Configuration

Example To enable the interface statistics counter, use the following commands:

```
awplus# configure terminal  
awplus(config)# service statistics interfaces counter
```

To disable the interface statistics counter, use the following commands:

```
awplus# configure terminal  
awplus(config)# no service statistics interfaces counter
```

Command changes Version 5.4.7-2.1: command added

show interface

Overview Use this command to display interface configuration and status.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show interface [<interface-list>]`

Parameter	Description
<code><interface-list></code>	The interfaces or ports to display. An interface-list can be: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where ‘10’ is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. The specified interfaces must exist.

Mode User Exec and Privileged Exec

Example To display configuration and status information for all interfaces, use the command:

```
awplus# show interface
```

To display configuration and status information for the loopback interface lo, use the command:

```
awplus# show interface lo
```

To display configuration and status information for br1, use the command:

```
awplus# show interface br1
```

To display configuration and status information for eth1, use the command:

```
awplus# show interface eth1
```


Output Figure 11-1: Example output from the **show interface** command:

```
awplus#show interface
Interface eth0
  Link is UP, administrative state is UP
  Hardware is Ethernet, address is ce7f.dc5d.b53e
  index 3 metric 1 mtu 1500
  current duplex full, current speed 1000, current polarity mdi
  configured duplex auto, configured speed auto, configured polarity auto
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 39994480, bytes 4659884105, dropped 0, multicast packets 0
    output packets 31645676, bytes 5366141711
    input average rate : 30 seconds 120.83 Kbps, 5 minutes 80.63 Kbps
    output average rate: 30 seconds 108.47 Kbps, 5 minutes 84.53 Kbps
    input peak rate 44.41 Mbps at 2020/06/19 03:00:07
    output peak rate 4.41 Mbps at 2020/06/25 01:05:51
  Time since last state change: 6 days 20:51:11
...
```

Figure 11-2: Example output from the **show interface lo** command:

```
awplus#show interface lo
Interface lo
  Link is UP, administrative state is UP
  Hardware is Loopback
  index 1 metric 1
  <UP,LOOPBACK,RUNNING>
  VRF Binding: Not bound
  SNMP link-status traps: Disabled
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
  Time since last state change: 8 days 19:41:47
```

Figure 11-3: Example output from the **show interface br** command:

```
awplus#show interface brl
Interface brl
  Link is UP, administrative state is UP
  Hardware is Bridge
  IPv6 address fe80::200:cdff:fe38:f7/64
  index 33555969 metric 1
  MAC ageing time 300
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
    input packets 1328, bytes 143605, dropped 0, multicast packets 0
    output packets 1847, bytes 218999, multicast packets 1 broadcast packets 3
    input average rate : 30 seconds 3.00 Kbps, 5 minutes 1.02 Kbps
    output average rate: 30 seconds 5.32 Kbps, 5 minutes 2.06 Kbps
    input peak rate 8.19 Kbps at 2017/11/13 05:09:59
    output peak rate 17.05 Kbps at 2017/11/13 05:11:23
  Time since last state change: 0 days 00:00:09
```

Figure 11-4: Example output from the **show interface eth1** command:

```
awplus#show interface eth1
Interface eth1
  Link is DOWN, administrative state is UP
  Hardware is Ethernet, address is 0000.cd38.026a
  index 12 metric 1 mtu 1500
  configured duplex auto, configured speed auto, configured polarity auto
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 11, bytes 5848
    input average rate : 30 seconds 0 bps, 5 minutes 0 bps
    output average rate: 30 seconds 0 bps, 5 minutes 0 bps
    output peak rate 2.48 Kbps at 2018/04/10 18:22:14
  Time since last state change: 7 days 22:56:59
```

Related commands

- [mtu](#)
- [show interface brief](#)
- [show interface status](#)

Command changes Version 5.4.7-2.1: average rate and peak rate added to output

show interface brief

Overview Use this command to display brief interface, configuration, and status information, including provisioning information.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show interface brief`

Mode User Exec and Privileged Exec

Example To display summarized information about all interfaces on the device, use the command:

```
awplus# show interface brief
```

Output Figure 11-5: Example output from **show interface brief**

```
awplus#show interface brief
Interface      Status        Protocol
eth0           admin up      running
eth1           admin up      running
eth2           admin up      running
eth3           admin up      running
eth3.108       admin up      down
eth3.104       admin up      down
...
lo             admin up      running
tunnel100      admin up      running
tunnel104      admin up      down
...
br0            admin up      down
br1            admin up      running
```

Table 11-1: Parameters in the output of **show interface brief**

Parameter	Description
Interface	The name or type of interface.
Status	The administrative state. This can be either admin up or admin down .
Protocol	The link state. This can be either down , running , or provisioned .

Related commands [show interface](#)
[show interface status](#)

show interface status

Overview Use this command to display the status of the specified interface or interfaces. Note that when no interface or interfaces are specified then the status of all interfaces on the device are shown.

Syntax `show interface [<port-list>] status`

Parameter	Description
<port-list>	The ports to display information about. The port list can be: - an Eth interface (e.g. eth0) - an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. - a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) - a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list.

Examples To display the status of eth0.2 and eth0.3, use the command:

```
awplus# show interface eth0.2,eth0.3 status
```

To display the status of all ports, use the command:

```
awplus# show interface status
```

Output

Table 12: Example output from the **show interface <port-list> status** command

awplus#show interface eth0.2,eth0.3 status					
Port	Name	Status	Vlan	Duplex	Speed Type
eth0.2	area2	connected	none	a-full	a-1000
eth0.3	area3	connected	none	a-full	a-1000

Table 13: Example output from the **show interface status** command

awplus#show interface status					
Port	Name	Status	Vlan	Duplex	Speed Type
eth0		connected	none	a-full	a-1000 1000BASE-T
eth0.3	area3	connected	none	a-full	a-1000
eth0.2	area2	connected	none	a-full	a-1000
...					

Table 14: Parameters in the output from the **show interface status** command

Parameter	Description
Port	Name/Type of the interface.
Name	Description of the interface.
Status	The administrative and operational status of the interface; one of: - disabled: the interface is administratively down. - connect: the interface is operationally up. - notconnect: the interface is operationally down.
Vlan	VLAN type or VLAN IDs associated with the port: When the port is an Eth port, it displays none: there is no VLAN associated with it.
Duplex	The actual duplex mode of the interface, preceded by a- if it has autonegotiated this duplex mode. If the port is disabled or not connected, it displays the configured duplex setting.
Speed	The actual link speed of the interface, preceded by a- if it has autonegotiated this speed. If the port is disabled or not connected, it displays the configured speed setting.
Type	The type of interface, e.g. 1000BaseTX.

Related commands [show interface](#)
[show interface brief](#)

shutdown

Overview This command shuts down the selected interface. This administratively disables the link and takes the link down at the physical (electrical) layer.

Use the **no** variant of this command to disable this function and bring the link back up again.

Syntax shutdown
no shutdown

Mode Interface Configuration

Example To shut down eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# shutdown
```

To bring up eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no shutdown
```

Part 2: Interfaces and Layer 2

12

Bridging Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure bridging. For more information, see the [Bridging Feature Overview and Configuration Guide](#).

- Command List**
- [“ageing-time”](#) on page 397
 - [“bridge”](#) on page 398
 - [“bridge-group”](#) on page 399
 - [“l3-filtering enable”](#) on page 401
 - [“mac-learning”](#) on page 402
 - [“show bridge”](#) on page 403
 - [“show bridge macaddr”](#) on page 405

ageing-time

Overview This command specifies the time period that a learned MAC address will remain defined within the bridge's MAC address table.

Use the **no** variant of this command to set the ageing out time back to the default.

Syntax ageing-time <10-1000000>
no ageing-time

Parameter	Description
<10-1000000>	The number of seconds that the MAC addresses will remain in the table.

Default 300 seconds (5 minutes)

Mode Interface Configuration

Examples To change the ageing time on br2 to 60 seconds (1 minute), use the following commands:

```
awplus#configure terminal
awplus(config)#interface br2
awplus(config-if)#ageing-time 60
```

To reset the ageing time back to its default, use the following commands:

```
awplus#configure terminal
awplus(config-if)#no ageing-time
```

To reset the ageing time back to its default, you can also use the following commands:

```
awplus#configure terminal
awplus(config-if)#ageing-time 300
```

Output None

Related commands [bridge](#)
[bridge-group](#)
[show bridge](#)
[show bridge macaddr](#)

bridge

Overview Use this command to create a software bridge.
Use the **no** variant of this command to remove the specified bridge.

Syntax `bridge <bridge-id>`
`no bridge <bridge-id>`

Parameter	Description
<code><bridge-id></code>	The bridge ID (from 1 to 300).

Default No configured bridges

Mode Global Configuration

Usage notes The bridge interface name will be prefixed with 'br' followed by the bridge ID.
*If interfaces exist on a bridge, then the bridge cannot be removed. For example if interface eth1 exists on bridge 2, then the **no bridge 2** command will give you the following message:*

```
% failed to remove interface br2, there are still configured sub-interfaces.
```

Example To create a bridge with the ID of 2, use the following commands:

```
awplus#configure terminal  
awplus(config)#bridge 2
```

To remove the bridge with the ID of 2, use the following commands:

```
awplus#configure terminal  
awplus(config)##no bridge 2
```

Related commands [ageing-time](#)
[bridge-group](#)
[show bridge](#)
[show bridge macaddr](#)

Command changes Version 5.5.4-0.1: maximum valid ID number changed to 300

bridge-group

Overview Use this command to add an interface to a bridge. Interfaces that have been added to a bridge will lose their L3 properties.

Use the **no** variant of this command to remove an interface from a bridge.

Syntax `bridge-group <0-255> [port-protected]`
`no bridge-group`

Parameter	Description
<0-255>	The ID of the bridge that you are adding the interface to. Interface ID 0 is a VLAN-aware bridge. For container services, allocate an interface ID of 0.
port-protected	Interfaces added to a bridge can be added in “protected” mode. Interfaces in this mode that are part of the same bridge-group will be unable to bridge to each other, but communication with unprotected interfaces will be unimpeded. Omitting this option from the command will add the interface in unprotected mode.

Default Interfaces do not belong to any bridges.

Mode Interface Configuration

Usage notes Interfaces can only be part of one bridge, so when removing the bridge no parameters are required.

Interfaces that have been added to a bridge will lose their Layer 3 properties. The bridge will act as the Layer 3 interface. The bridge will provide Layer 2 connectivity between interfaces that are a part of the same bridge-group.

You can attach interfaces such as Ethernet and VTI (Tunnel) to your bridge.

Examples To add eth0 to bridge 2 in unprotected mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# bridge-group 2
```

To add eth0 to bridge 2 in protected mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# bridge-group 2 port-protected
```

To remove eth0 from bridge 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no bridge-group
```

**Related
commands**

[ageing-time](#)
[bridge](#)
[show bridge](#)
[show bridge macaddr](#)

l3-filtering enable

Overview Use this command to enable traffic control for bridged traffic on a bridge interface. Use the **no** variant of this command to disable traffic control for bridged traffic on a bridge interface.

Syntax `l3-filtering enable`
`no l3-filtering enable`

Default Traffic control is disabled by default for bridged traffic.

Mode Interface mode for a bridge interface

Usage notes We do not recommend shaping bridged traffic on firewalls that are running Unified Threat Management (UTM) features, because both Traffic Control and UTM require significant CPU resources.

Example To enable traffic control for bridged traffic on br1, use the commands:

```
awplus# configure terminal
awplus(config)# interface br1
awplus(config-if)# l3-filtering enable
```

Related commands [traffic-control](#)

Command changes Version 5.4.7-0.1: command added. Previously, traffic control was enabled by default on all bridge interfaces.

mac-learning

Overview Use this command to enable FDB MAC address learning on a bridge interface. In some circumstances, FDB MAC address learning on a software-based router bridge is not useful, and it is better to flood the traffic within interfaces associated with the bridge instance, to ensure the traffic reaches its destination.

Use the **no** variant of this command to disable or enable FDB MAC address learning on a bridge.

Syntax `mac-learning`
`no mac-learning`

Default Learning is enabled by default.

Mode Interface mode for a bridge interface

Example To turn off learning on bridge 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface br2
awplus(config-if)# no mac-learning
```

To turn learning on bridge 2 back on, use the following commands:

```
awplus# configure terminal
awplus(config)# interface br2
awplus(config-if)# mac-learning
```

Command changes Version 5.4.7-0.1: command added

show bridge

Syntax Use this command to display detailed information about your bridge(s).

Syntax `show bridge [<bridge-list>]`

Parameter	Description
<bridge-list>	The bridge/s to display the information about. The <bridge-list> can be: • a single bridge(e.g. br2) • a continuous range of bridges (e.g. br1-3) • a comma separated list of bridges and/or ranges (e.g. br1,br2,br3-br5)

Default Displays detailed information about all bridges, if no <bridge-list> is specified.

Mode Privileged Exec

Examples To display information about all bridges, use the following command:

```
awplus#show bridge
```

To display information about bridge 2, use the following command:

```
awplus#show bridge br2
```

To display information about bridge in the range 1 to 3, use the following command:

```
awplus#show bridge br1-3
```

To display information about bridges 1, and from 3 to 5, use the following command:

```
awplus#show bridge br1,br3-5
```

Output Figure 12-1: Example output from the **show bridge** command displaying information about all bridges:

awplus#show bridge		
Bridge Name	Aging Timer	Interfaces

br1	300	eth1
br3	300	
br4	300	
br5	300	

Figure 12-2: Example output from the **show bridge** command displaying information about bridge 1.

```
awplus#show bridge br1
Bridge Name      Aging Timer      Interfaces
-----
br1              300              eth1
```

**Related
commands**

[ageing-time](#)
[bridge](#)
[bridge-group](#)
[show bridge macaddr](#)

show bridge macaddr

Overview Use this command to display the MAC entries learned in the MAC table for your bridge.

Syntax `show bridge macaddr <bridge-list>`

Parameter	Description
<bridge-list>	The bridge interfaces to display the information about. The <bridge-list> can be: • a single bridge (e.g. br2) • a continuous range of bridges (e.g. br1-3) • a comma separated list of bridges and/or ranges (e.g. br1,br2,br3-br5)

Mode Global Configuration

Example To display the learned MAC entries for bridge 2, use the following commands:

```
awplus# configure terminal
awplus(config)# show bridge macaddr br2
```

Output Figure 12-3: Example output from the **show bridge macaddr** command displaying information about bridge 2:

awplus#show bridge macaddr br2				
Bridge Name	Interface	mac addr	is local?	ageing

br2	eth0	ec:cd:6d:20:c0:fb	no	41
br2	eth0	00:c4:6d:20:c0:e6	no	0
br2	eth0	ec:cd:6d:20:c0:bd	yes	0
...				

Related commands

- [ageing-time](#)
- [bridge](#)
- [bridge-group](#)
- [show bridge](#)

13

802.1Q Encapsulation Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure 802.1Q Encapsulation. For more information, see the [Interface Feature Overview and Configuration Guide](#).

Command List • [“encapsulation dot1q”](#) on page 407

encapsulation dot1q

Overview Use this command to enable 802.1Q encapsulation on Ethernet interfaces, L2 tunnel interfaces (e.g. OpenVPN or L2TPv3 Ethernet pseudowire), or the VLAN-aware bridge 0.

Use the **no** variant of this command to disable 802.1Q encapsulation for the VLAN identified by the VLAN ID (VID).

Syntax `encapsulation dot1q <vid>`
`no encapsulation dot1q <vid>`

Parameter	Description
<vid>	Enter a VLAN ID in the range from 1 through 4094. The VLAN ID identifies the VLAN to which the frames belong. It also identifies the index of the subinterface of the Ethernet interface or Layer 2 tunnel interface.

Default 802.1Q encapsulation is disabled by default on all Ethernet interfaces, Layer 2 tunnel interfaces, and bridge interfaces.

Mode Interface Configuration

Usage notes You should enter the Ethernet interface or tunnel interface configuration mode to enable 802.1Q encapsulation and configure the VID first. Then you can use the VID to configure the sub-interface associated with the Ethernet interface or tunnel interface. Sub-interfaces are logical interfaces. The sub interface index must be the same as the VID. For example, if you configure VID 1 for eth1, then the sub-interface for eth1 is eth1.1. If you configure VID 2 for tunnel20, then the sub-interface for tunnel20 is tunnel20.2.

Examples To enable 802.1Q encapsulation on Ethernet interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# encapsulation dot1q 1
```

To enable 802.1Q encapsulation on tunnel interface tunnel20, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel20
awplus(config-if)# encapsulation dot1q 2
```

To enable multiple 802.1Q encapsulation on Ethernet interface eth0, use the commands:

```
awplus# configure terminal
awuplus(config)# interface eth0
awplus(config-if)# encapsulation dot1q 1
awplus(config-if)# encapsulation dot1q 2
awplus(config-if)# encapsulation dot1q 3
```

To disable 802.1Q encapsulation on eth0, use the commands:

```
awplus# configure terminal
awuplus(config)# interface eth0
awuplus(config-if)# no encapsulation dot1q 1
```

Related commands [interface \(to configure\)](#)
[show interface](#)

14

PPP Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure and validate the PPP (Point-To-Point) protocol. For more information about PPP, see the [Point-to-Point Protocol \(PPP\) Feature Overview and Configuration Guide](#).

- Command List**
- [“debug ppp”](#) on page 411
 - [“encapsulation ppp”](#) on page 414
 - [“interface \(PPP\)”](#) on page 415
 - [“ip address negotiated”](#) on page 416
 - [“ip tcp adjust-mss”](#) on page 418
 - [“ip unnumbered”](#) on page 420
 - [“ipv6 tcp adjust-mss”](#) on page 422
 - [“keepalive \(PPP\)”](#) on page 424
 - [“mtu \(PPP\)”](#) on page 426
 - [“peer default ip address”](#) on page 427
 - [“peer neighbor-route”](#) on page 429
 - [“ppp authentication”](#) on page 431
 - [“ppp authentication refuse”](#) on page 433
 - [“ppp hostname”](#) on page 435
 - [“ppp ipcp dns”](#) on page 437
 - [“ppp ipcp dns suffix-list”](#) on page 439
 - [“ppp ipcp ip-override”](#) on page 441
 - [“ppp password”](#) on page 442
 - [“ppp service-name \(PPPoE\)”](#) on page 443

- [“ppp timeout idle”](#) on page 444
- [“ppp username”](#) on page 445
- [“show debugging ppp”](#) on page 446
- [“show interface \(PPP\)”](#) on page 447
- [“undebg ppp”](#) on page 451

debug ppp

Overview Use this command to enable PPP protocol debugging on an optionally specified PPP interface or range of PPP interfaces to analyze PPP behavior when diagnosing PPP connectivity issues. If no interface is specified then debugging for all PPP interfaces is enabled.

Use the **no** variant of this command to disable PPP protocol debugging on the specified PPP interface. If no PPP interface is specified then PPP debugging for all PPP interfaces is disabled.

Syntax `debug ppp [interface <ppp-interface-list>]`
`no debug ppp [interface <ppp-interface-list>]`

Parameter	Description
<ppp-interface- list>	Specify a PPP interface or a range of PPP interfaces in the range ppp<0-255>. Use a hyphen between PPP interfaces to include all PPP interfaces in a given range, or use commas between PPP interfaces to specify non-contiguous PPP interfaces.

Default No diagnostic messages are enabled for PPP debugging. PPP debugging is disabled by default.

Mode Global Configuration and Privileged Exec

Usage notes Debugging messages are sent to the logging system and can be viewed in log output, filtered in permanent or buffered logs, and viewed on the terminal using the [terminal monitor](#) command. See the status of PPP debugging with the [show debugging ppp](#) command.

Note that debugging output for PPP shows packet debugging and events debugging, see output below.

Note that disabling all debugging with the [no debug all](#) or the [undebug all](#) commands also disables PPP debugging configured with this command.

Note that the negated form of this command is an alias of the [undebug ppp](#) command.

Examples To enable PPP debugging on all PPP interfaces and send diagnostic messages to the system log, use the below command:

```
awplus# debug ppp
```

To enable PPP debugging on PPP interfaces ppp0 through ppp2 and display them on the console, use the below commands:

```
awplus# terminal monitor
```

```
awplus# debug ppp interface ppp0-ppp2
```

Output of packet debugging

Figure 14-1: Example output from the **debug ppp** command on the console

```
awplus#terminal monitor
awplus#debug ppp

05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.901] sent [IPCP
ConfReq id=0x1 <addr
0.0.0.0> <ms-dns1 0.0.0.0> <ms-dns2 0.0.0.0>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.901] sent [IPV6CP
ConfReq id=0x1
<addr fe80::eecd:6dff:fe3a:0d23>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.901] rcvd [LCP
ConfAck id=0x1 <magic
0xd9153444>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.919] rcvd [IPCP
ConfReq id=0x1 <addr
192.168.1.1>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.919] sent [IPCP
ConfAck id=0x1 <addr
192.168.1.1>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.919] rcvd [IPCP
ConfNak id=0x1 <addr
192.168.1.2> <ms-dns1 1.1.1.1> <ms-dns2 2.2.2.2>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.920] sent [IPCP
ConfReq id=0x2 <addr
192.168.1.2> <ms-dns1 1.1.1.1> <ms-dns2 2.2.2.2>]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.921] rcvd [LCP
ProtRej id=0x2 80 57
01 01 00 0e 01 0a ee cd 6d ff fe 3a 0d 23]
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.921] Protocol-Reject
for 'IPv6
Control Protocol' (0x8057) received
05:35:46 awplus pppd[24767]: [ppp0] [05:35:46.922] rcvd [IPCP
ConfAck id=0x2 <addr
192.168.1.2> <ms-dns1 1.1.1.1> <ms-dns2 2.2.2.2>]
02:25:35 awplus pppd[2388]: [ppp1] [02:25:35.990] sent [LCP
EchoReq id=0x3b
magic=0xe1e041db]
02:25:35 awplus pppd[2388]: [ppp1] [02:25:35.991] rcvd [LCP
EchoReq id=0x3b
magic=0xe3e331b1]
02:25:35 awplus pppd[2388]: [ppp1] [02:25:35.991] sent [LCP
EchoRep id=0x3b
magic=0xe1e041db]
02:25:35 awplus pppd[2388]: [ppp1] [02:25:35.992] rcvd [LCP
EchoRep id=0x3b
magic=0xe3e331b1]
```


Output of event debugging

Figure 14-2: Example output from the **debug ppp** command for a PPP interface

```
awplus#terminal monitor
awplus#debug ppp interface ppp0

05:35:43 awplus pppd[24767]: [ppp0] [05:35:43.710] using channel 1
05:35:43 awplus pppd[24767]: [ppp0] [05:35:43.712] Using interface
ppp0
05:35:43 awplus pppd[24767]: [ppp0] [05:35:43.712] Connect: ppp0
<--> hdlc0
05:35:46 awplus PPP: IP is up on interface ppp0 [local-IP:
192.168.1.2, remote-IP:
192.168.1.1]
05:35:46 awplus PPP: IPCP [ppp0]: add IP interface [IP-addr:
192.168.1.2, mask: ]
05:35:46 awplus PPP: IPCP [ppp0]: add host route [peer-IP:
192.168.1.1]
05:35:47 awplus PPP: IPCP [ppp0]: add domain name server [DNS:
1.1.1.1]
05:35:47 awplus PPP: IPCP [ppp0]: add domain name server [DNS:
2.2.2.2]
```

To record messages relating to PPP packets in the buffered log, first configure a buffered log filter to select the messages using the commands:

```
awplus# configure terminal
awplus(config)# log buffered level debug program pppd
awplus(config)# end
```

Then configure PPP debugging, using the below command:

```
awplus# debug ppp
```

To disable PPP debugging for all PPP interfaces, use the below command:

```
awplus# no debug ppp
```

Related commands

- [terminal monitor](#)
- [encapsulation ppp](#)
- [no debug all](#)
- [ppp authentication](#)
- [show debugging ppp](#)
- [show interface \(PPP\)](#)
- [undebug all](#)

encapsulation ppp

Overview Use this command to enable PPP encapsulation and create one or more PPP interfaces over Ethernet, a cellular interface, or an L2TPv2 managed VPN.

Use the **no** variant of this command to disable PPP encapsulation and remove the specified PPP interface.

Syntax `encapsulation ppp <index>`
`no encapsulation ppp <index>`

Parameter	Description
<index>	The PPP interface index number in the range from 0 to 255.

Default No PPP encapsulation or interfaces are configured by default.

Mode Interface Configuration mode for an Ethernet interface (e.g. **interface eth1**) or an Ethernet sub-interface (e.g. **interface eth1.1**).

Examples To configure a PPP interface with index 0 for Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# encapsulation ppp 0
```

To shut down the ppp0 interface and remove it from Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# shutdown
awplus(config-if)# interface eth1
awplus(config-if)# no encapsulation ppp 0
```

Related commands [ppp service-name \(PPPoE\)](#)
[show interface \(PPP\)](#)

interface (PPP)

Overview Use this command to select a PPP interface to configure.

You need to use the [encapsulation ppp](#) command to enable PPP encapsulation and create PPP interfaces first.

Syntax `interface <PPP-interface-list>`

Parameter	Description
<code><PPP-interface-list></code>	The PPP interfaces or ports to configure. An interface-list can be: • a PPP interface (e.g. ppp0) • a continuous range of PPP interfaces, separated by a hyphen (e.g. ppp0-ppp2) • a comma-separated non-continuous list of PPP interfaces (e.g. ppp0, ppp2) The specified interfaces must exist.

Mode Global Configuration

Example The following example shows how to enter Interface mode to configure a PPP interface.

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)#
```

Related commands [ip address \(IP Addressing and Protocol\)](#)
[show interface](#)
[show interface brief](#)

ip address negotiated

Overview Use this command to obtain an IP address with the peer for a PPP interface via IPCP (Internet Protocol Control Protocol) address negotiation when configuring a PPP link for IP traffic.

Use the **no** variant of this command to remove IP address negotiation settings.

Syntax `ip address negotiated [<default-ip-address>]`
`no ip address negotiated`

Parameter	Description
<code><default-ip-addr></code>	Specify an optional default IP address for use instead of an IP address assigned from the peer that is otherwise configured for a PPP interface.

Default No IP address negotiation with the peer is configured by default.

Mode Interface Configuration for a PPP interface

Usage notes Use this command to enable the device to automatically negotiate an IP address for a PPP interface, and to enable all remote hosts to access the device using this IP address. When the peer does not send an IP address via IPCP negotiation, the specified default IP address will be used.

Examples To configure the PPP interface ppp0 to use IPCP to negotiate an IP address for itself, use the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip address negotiated
```

To configure the PPP interface ppp0 to a default IP address of 10.9.9.2, for use when the peer does not send an IP address via IPCP negotiation, use the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip address negotiated 10.9.9.2
```

To stop the PPP interface ppp0 from using IPCP to negotiate an IP address for itself, use the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip address negotiated
```

Output To verify IPCP address negotiation is configured on PPP interface ppp0, use the following command:

```
awplus# show running-config interface ppp0
```

Figure 14-3: Example output from **show running-config interface ppp0** to verify IPCP configuration:

```
!  
interface ppp0  
  ip address negotiated  
!
```

Related commands

- [show ip interface](#)
- [encapsulation ppp](#)
- [peer default ip address](#)
- [show running-config interface](#)

ip tcp adjust-mss

Overview Use this command to set the Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

Syntax `ip tcp adjust-mss {<mss-size>|pmtu}`
`no ip tcp adjust-mss`

Parameter	Description
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	Adjust TCP MSS automatically with respect to the MTU on the interface.

Default The default setting allows a TCP server or a TCP client to set the MSS value for itself.

Mode Interface Configuration

Usage notes When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel

Examples To configure an MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ip tcp adjust-mss 1452
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip tcp adjust-mss
```

**Related
commands**

[mtu \(PPP\)](#)
[show interface](#)
[show interface \(PPP\)](#)

**Command
changes**

Version 5.4.8-2.1: interface tunnel example added

ip unnumbered

Overview Use this command to borrow an IP address from the specified interface, on an unnumbered PPP interface.

Use the **no** variant of this command to remove the borrowed IP address.

Syntax `ip unnumbered <interface-name>`
`no ip unnumbered`

Parameter	Description
<code><interface-name></code>	Name of the interface from which the IP address is to be borrowed. Valid interface types from which the IP address can be borrowed are Ethernet, loopback, and bridge.

Default IP unnumbered is disabled by default.

Mode Interface Configuration for a PPP interface

Usage notes An unnumbered PPP interface can process IP packets without explicitly assigning an IP address. This is achieved by borrowing the primary IP address from the specified Ethernet, loopback, or bridge interface.

Examples To borrow an IP address on unnumbered PPP from Eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip address 6.6.6.6/24
awplus(config-if)# exit
awplus(config)# interface ppp0
awplus(config-if)# ip unnumbered eth1
```

To remove the borrowed IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip unnumbered
```

To verify borrowed address is configured on PPP interface ppp0, use the following command:

```
awplus# show interface ppp0
```


Figure 14-4: Example output from a **show interface** ppp0 to verify PPP IP borrowing configuration:

```
awplus#show interface ppp0
Interface ppp0
  Link is UP, administrative state is UP
  Hardware is PPP
  Interface is unnumbered. Using IPv4 address of eth1 (2.2.2.2)
  index 16778240 metric 1 mtu 1492
  <UP,POINT-TO-POINT,RUNNING,NOARP,MULTICAST>
  PPP is running over interface eth1
  LCP Opened IPCP Opened
  MRU(bytes): Local config 1492, Local negotiated 1492, Peer
  negotiated 1492
  Magic number: Local config ON, Local negotiated ON, Peer
  negotiated ON
  Authentication: Local config None, Local neg None, Peer neg CHAP
  IPv4 addresses: Local config 0.0.0.0
                  Local neg 2.2.2.2, Peer neg 1.1.1.1
  IPv6 Id Local config: 0000:0000:0000:0000
  PPPoE is using the default service
  SNMP link-status traps: Disabled
    input packets 2, bytes 20, dropped 0, multicast packets 0
    output packets 2, bytes 20, multicast packets 0 broadcast
    packets 0
  Time since last state change: 0 days 00:00:13
```

Related commands [show ip interface](#)
 [show running-config interface](#)

ipv6 tcp adjust-mss

Overview Use this command to set the IPv6 Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

Syntax `ipv6 tcp adjust-mss {<mss-size>|pmtu}`
`no ipv6 tcp adjust-mss`

Parameter	Description
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	Adjust TCP MSS automatically with respect to the MTU on the interface.

Default The default setting allows a TCP server or a TCP client to set the MSS value for itself.

Mode Interface Configuration

Usage notes When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel

Examples To configure an IPv6 MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To configure an IPv6 MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To adjust IPv6 TCP MSS automatically with respect to the MTU on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ipv6 tcp adjust-mss pmtu
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 tcp adjust-mss
```

**Related
commands**

[mtu \(PPP\)](#)
[show interface](#)
[show interface \(PPP\)](#)
[show interface tunnel \(GRE\)](#)

**Command
changes**

Version 5.4.8-2.1: interface tunnel example added

keepalive (PPP)

Overview Use this command to enable LCP (Link Control Protocol) Echo keepalive request messages and change LCP echo parameters on a given PPP interface in Interface Configuration mode.

Use the **no** variant of this command to disable LCP Echo keepalive request messages on a given PPP interface in Interface Configuration mode. Note that disabling the sending of LCP Echo keepalive request messages does not stop a device responding to LCP Echo requests.

Syntax `keepalive [[interval <interval>] [attempts <attempt-limit>]]no keepalive`

Parameter	Description
<interval>	Specify the interval in seconds in the range <1–600> seconds between LCP Echo keepalive request messages, for a PPP interface. Default: 10
<attempt-limit>	Specify the number of missing LCP Echo keepalive response messages, in the range <1–10> for a PPP interface, before the link is considered as being link down and link renegotiation starts to reestablish the link. Default: 3

Default The sending of LCP Echo keepalive messages on a PPP interface is disabled by default. If no optional **interval** is specified then the default interval duration is configured to 10 seconds. If no optional **attempts** are specified then the default attempt limit is configured to 3 attempts.

Mode Interface Configuration for a PPP interface

Example To enable the device to send LCP Echo keepalive messages on the PPP interface `ppp0` with the default 10 second interval when no interval is specified and the default 3 attempts when no attempt is specified, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# keepalive
```

To enable the device to send LCP Echo keepalive messages on the PPP interface `ppp0` with double the default values for a 20 second interval and 6 attempts, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# keepalive interval 20 attempts 6
```

To disable the device from sending LCP Echo keepalive messages on the PPP interface `ppp0`, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no keepalive
```

Related commands [show running-config interface](#)

mtu (PPP)

Overview Use this command to set the Maximum Transmission Unit (MTU) size for a PPP interface, where MTU is the maximum packet size that PPP interfaces can transmit.

Use the **no** variant of this command to remove a previously specified MTU size for a PPP interface, and restore the default MTU size (1492 bytes) for PPP interfaces.

Syntax `mtu <mtu-size>`
`no mtu`

Parameter	Description
<code><mtu-size></code>	<code><68-1492></code> Specifies the Maximum Transmission Unit (MTU) size in bytes, where 1492 bytes is the default MTU size for a PPPoE interface and 1500 bytes for PPP via other lower layer interface types. This allows for the 8-byte PPPoE header that is added to make up the total of a 1582 byte packet that matches the default MTU size for the Ethernet link..

NOTE: For PPPoE the minimum MTU value is 128.

Default The default MTU size is 1492 bytes for PPPoE interfaces. The MTU should be greater than, or equal to, the MSS.

Mode Interface Configuration for PPP interfaces.

Usage notes If a router receives an IPv4 packet for another PPP interface with an MTU size smaller than the packet size, and if the packet has the '**don't fragment**' bit set, then the switch will send an ICMP '**destination unreachable**' (3) packet type and a '**fragmentation needed and DF set**' (4) code back to the source.

See the [ip tcp adjust-mss](#) command to set the Maximum Segment Size (MSS) after first setting the MTU size.

Examples To configure an MTU size of 1492 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# mtu 1492
```

To restore the MTU size to the default MTU size of 1492 bytes on PPP interface ppp0, use the commands

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no mtu
```

Related commands [ip tcp adjust-mss](#)
[show interface \(PPP\)](#)

peer default ip address

Overview Use this command to set the default IP address assigned to the peer if required for a given PPP interface.

Use the optional **required** keyword with this command to specify that the peer must use this address for a given PPP interface, or drop the connection.

Use the **no** variant of this command to remove the previously specified peer default IP address for a given PPP interface.

Syntax peer default ip address <default-ip-address> [required]
no peer default ip address

Parameter	Description
<default-ip-address>	Specify the IPv4 address to be assigned to the peer upon request.
required	Optionally specify the peer to acknowledge the default IP address, which requires the peer to use the address or drop the connection.

Default No default IP address is configured to be assigned to the peer.

Mode Interface Configuration for a PPP interface

Examples To configure the PPP interface ppp0 to assign the IP address of 192.168.0.1 to its peer upon request, use the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# peer default ip address 192.168.0.1
```

To configure the PPP interface ppp0 to have the default peer IP address of 192.168.0.1, and be required to use it or drop the connection, use the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# peer default ip address 192.168.0.1
required
```

To remove the default peer IP address of 192.168.0.1 from the PPP interface ppp0, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no peer default ip address
```

To verify the required peer default IP address 192.168.0.1 is configured on PPP interface ppp0, use the following command:

```
awplus# show running-config interface ppp0
```

Related commands [ip address negotiated](#)
[show running-config interface](#)

peer neighbor-route

Overview Use this command in Interface Configuration mode for a PPP interface to re-enable the creation of peer neighbor routes after the default behavior has been disabled.

Use the **no** form of this command in Interface Configuration mode for a PPP interface to disable the default behavior of creating a neighbor route for the peer.

Syntax `peer neighbor-route`
`no peer neighbor-route`

Default A 32-bit host route (with a /32 mask) is created to the peer address on a PPP interface after PPP IPCP negotiation finishes.

Usage notes Use the **no** form of this command if the default behavior creates issues within your network. Use the [show ip route](#) command to validate the route behavior after issuing this command.

Mode Interface Configuration for a PPP interface

Examples To re-enable the default behavior for the PPP interface `ppp1`, where a 32-bit host route (with a /32 mask) is created to the peer address on a PPP interface after PPP IPCP negotiation finishes, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp1
awplus(config-if)# peer neighbor-route
```

To disable the default behavior for the PPP interface `ppp0`, to prevent a 32-bit host route being added to the IP router table, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no peer neighbor-route
```

Related commands [show interface \(PPP\)](#)
[show ip route](#)

Output Figure 14-5: Example validation output from the **show interface** and **show ip route** commands issued before and after the **no peer neighbor-route** command (see IPv4 address in **show interface** output and see connected routes **show ip route** output):

```
awplus#show interface ppp1
Interface ppp1
  Scope: both
  Link is UP, administrative state is UP
  Hardware is PPP
  IPv4 address 4.1.1.2/32 pointopoint 4.1.1.1
  index 16778241 metric 1 mtu 1460
  <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
  VRF Binding: Not bound
  PPP is running over interface tunnel1
  LCP Opened IPCP Opened
  L2TP session ID is 59451
  SNMP link-status traps: Disabled
    input packets 5, bytes 66, dropped 0, multicast packets 0
    output packets 4, bytes 46, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 00:02:24
awplus#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       *- candidate default

C       4.1.1.1/32 is directly connected, ppp1
C       4.1.1.2/32 is directly connected, ppp1
C       192.168.10.0/24 is directly connected, vlan1
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#interface ppp1
awplus(config-if)#no peer neighbor-route
awplus(config-if)#exit
awplus(config)#exit
awplus#show interface ppp1
Interface ppp1
  Scope: both
  Link is UP, administrative state is UP
  Hardware is PPP
  IPv4 address 4.1.1.2/32
  index 16778241 metric 1 mtu 1460
  <UP,POINTOPOINT,RUNNING,NOARP,MULTICAST>
  VRF Binding: Not bound
  PPP is running over interface tunnel1
  LCP Opened IPCP Opened
  L2TP session ID is 6262
  SNMP link-status traps: Disabled
    input packets 5, bytes 66, dropped 0, multicast packets 0
    output packets 4, bytes 46, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 00:00:09
awplus#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       *- candidate default

C       4.1.1.2/32 is directly connected, ppp1
C       192.168.10.0/24 is directly connected, vlan1
```

ppp authentication

Overview Use this command in Interface Configuration mode for a PPP interface to configure PAP (Password Authentication Protocol), CHAP (Challenge Authentication Protocol), or EAP (Extensible Authentication Protocol).

Use the **no** form of this command in Interface Configuration mode for a PPP interface to disable all PAP, CHAP, and EAP authentication for a specified PPP interface.

Syntax `ppp authentication {eap|chap|pap}`
`no ppp authentication`

Parameter	Description
eap	Specify this parameter to enable EAP on a PPP interface
chap	Specify this parameter to enable CHAP on a PPP interface.
pap	Specify this parameter to enable PAP on a PPP interface.

Default There is no PPP authentication protocol defined or configured to a PPP interface by default.

Mode Interface Configuration for a PPP interface

Examples To enable PPP PAP authentication on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication pap
```

To enable PPP CHAP authentication on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication chap
```

To enable PPP EAP authentication on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication eap
```

To attempt PPP EAP authentication, then fall back to PPP CHAP authentication if the attempt to enable PPP EAP authentication fails on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication eap chap
```

To attempt PPP CHAP authentication, then fall back to PPP PAP authentication if the attempt to enable PPP CHAP authentication fails on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication chap pap
```

To disable all PPP authentication on the PPP interface `ppp0`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp authentication
```

Related commands

- [ppp authentication refuse](#)
- [ppp hostname](#)
- [ppp password](#)
- [ppp username](#)

ppp authentication refuse

Overview Use this command in Interface Configuration mode for a PPP interface to refuse EAP, CHAP (Challenge Handshake Authentication Protocol) or PAP (Password Authentication Protocol) authentication from peers requesting it.

Use the **no** form of this command in Interface Configuration mode for a PPP interface to allow authentication from peers requesting it.

Syntax `ppp authentication refuse {eap|chap|pap}`
`no ppp authentication refuse`

Parameter	Description
eap	Use this parameter to specify the router will refuse LCP configuration requests containing the authentication protocol option with EAP received on this PPP interface.
chap	Use this parameter to specify the router will refuse LCP configuration requests containing the authentication protocol option with CHAP received on this PPP interface.
pap	Use this parameter to specify the router will refuse LCP configuration requests containing the authentication protocol option with PAP on this PPP interface.

Mode Interface Configuration for a PPP interface

Usage notes This command specifies that EAP, CHAP or PAP authentication is disabled, so all requests by the peer for the user to authenticate using EAP, CHAP or PAP are refused.

Examples To refuse the use of PAP authentication if a peer requests PAP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication refuse pap
```

To refuse the use of CHAP authentication if a peer requests CHAP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication refuse chap
```

To refuse the use of EAP authentication if a peer requests EAP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp authentication refuse eap
```

To allow the use of EAP, CHAP or PAP authentication if a peer requests EAP, CHAP or PAP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp authentication refuse
```

Related commands [ppp authentication](#)

ppp hostname

Overview Use this command in Interface Configuration mode for a PPP interface to configure a unique identifier for that PPP authenticator. This is used by the authenticator to fill the Name field in a CHAP challenge packet, or is used to fill the Server Name field in an EAP SRP-SHA1 (Subtype 1 Request) packet. The hostname sent with PPP packet exchanges is normally the hostname of the router, as configured with the [hostname](#) command.

Use the **no** form of this command in Interface Configuration mode for a PPP interface to disable a configured alternate hostname and revert to using the hostname, as configured with the [hostname](#) command.

See the Usage section below for information about when you may want to specify another hostname, instead of the system hostname configured from the [hostname](#) command, using this command.

Syntax `ppp hostname <hostname>`
`no ppp hostname <hostname>`

Parameter	Description
<code><hostname></code>	Specify this parameter to use an alternate hostname for PPP EAP and CHAP authentication instead of the hostname specified by the hostname command. The name can contain up to 255 characters. The name can contain any printable ASCII characters (ASCII 32-126). If the name contains the special characters backslash, double-quote or space, those characters should be escaped with a backslash.

Default The default PPP hostname is the system hostname as specified with the [hostname](#) command.

Mode Interface Configuration for a PPP interface

Usage notes This command allows the PPP username that is sent to be independent of the router hostname for a specific PPP interface.

Examples To enable the use of the alternate hostname `remote_router` for PPP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp hostname remote_router
```

To disable the use of the alternate hostname `remote_router` for PPP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp hostname remote_router
```

Related commands [hostname](#)
[ppp authentication](#)

ppp ipcp dns

Overview Use this command to configure the primary and secondary DNS (Domain Name System) IP addresses for IPCP (Internet Protocol Control Protocol) on a given PPP interface.

Use the **no** variant of this command to remove the primary and secondary DNS IP addresses for IPCP on a given PPP interface, and remove any optional parameters configured for DNS.

Syntax `ppp ipcp dns [<primary> [<secondary>]] [required|reject|request]`
`no ppp ipcp dns`

Parameter	Description
<code><primary></code>	Specify the primary DNS address for a given PPP interface to the peer.
<code><secondary></code>	Specify the secondary DNS address for a given PPP interface to the peer.
<code>required</code>	Request DNS addresses from the peer, and close the link if none is given.
<code>reject</code>	Reject negotiations with the peer (default).
<code>request</code>	Request DNS addresses from the peer.

Default By default no IPCP DNS server request is sent to the peer.

Mode Interface Configuration

Usage notes Use the optional parameters to configure PPP IPCP DNS options for accepting, rejecting or requesting DNS addresses from the peer. Use the optional primary and secondary or primary only DNS server address placeholders to specify DNS server addresses to the peer.

The no variant of this command also stops IPCP DNS request messages being sent to the peer.

Examples To configure the PPP interface `ppp0` to require a DNS IP address from the peer, and close the link if a DNS IP address is not given, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns required
```

To configure the PPP interface `ppp0` to require a DNS IP address from the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns request
```

To configure the PPP interface `ppp0` to reject a DNS IP address from the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns reject
```

To configure the PPP interface `ppp0` to supply primary and secondary DNS server addresses to the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns 10.1.1.2 10.1.1.3
```

To configure the PPP interface `ppp0` to supply a primary but not a secondary DNS server address to the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns 10.1.1.2
```

**Related
commands**

[ip address negotiated](#)
[peer default ip address](#)
[peer neighbor-route](#)
[show running-config interface](#)

ppp ipcp dns suffix-list

Overview Use this command to configure a suffix-list to be associated with DNS name-servers learned over the PPP connection.

Use the **no** variant of this command to remove the suffix-list.

Syntax `ppp ipcp dns suffix-list <domain-list-name>`
`no ppp ipcp dns suffix-list`

Parameter	Description
<code><domain-list-name></code>	The name of the DNS domain-list

Mode Interface Configuration

Usage notes A PPP connection can be configured to learn DNS servers from the remote peer by using the command `ppp ipcp dns` command.

This command allows a user to associate a domain-list to be used to match against the suffixes of incoming DNS requests. For example, a customer branch office may have a router that is used to give remote-access to their head office, over which they learn the IP address of the head office's DNS server. A domain list can be created that contains a suffix used for services internal to that company, for example, "example.lc". This domain-list is associated as a suffix-list to the PPP connection. So when the PPP connection is completed with the head office, users at the branch office that browse to "intranet.example.lc" will have the DNS request forwarded to the DNS server learned over the PPP connection. Without having the suffix-list configured, the DNS request for "intranet.example.lc" would instead be sent to the primary DNS server, which is likely to be the branch office's ISP, and they will simply respond with a negative reply, because .example.lc is not a globally routable domain.

Examples At a branch office, to direct DNS lookups for domains with suffixes of "engineering.acme" or "intranet.acme" to an internal corporate name-server run at head-office that was learned over a PPP connection, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
host(config-domain-list)# description Our internal network
domains; do not send DNS requests to internet
host(config-domain-list)# domain engineering.acme
host(config-domain-list)# domain intranet.acme
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns required
awplus(config-if)# ppp ipcp dns suffix-list corporatedomains
```

**Related
commands** [ip dns forwarding domain-list](#)
[ppp ipcp dns](#)

ppp ipcp ip-override

Overview Use this command to override the IP address negotiated via IPCP with peer and use the statically configured address on a given PPP interface.

Use the **no** variant of this command to use any address negotiated with the peer via IPCP on a given PPP interface.

Syntax `ppp ipcp ip-override`
`no ppp ipcp ip-override`

Default By default the address is negotiated with the peer via IPCP.

Mode Interface Configuration

Examples To override the IP address negotiated with the peer via IPCP and use statically configured address on interface ppp0, use the commands below:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip address 192.168.1.100/24
awplus(config-if)# ppp ipcp ip-override
```

Related commands [show running-config interface](#)

ppp password

Overview Use this command in Interface Configuration mode for a PPP interface to configure a PPP secret password to be used in response to a challenge from an unknown remote peer.

Use the **no** form of this command in Interface Configuration mode for a PPP interface to disable a configured PPP secret password.

Syntax `ppp password <password>`
`no ppp password`

Parameter	Description
<code><password></code>	Specify this parameter to configure a PPP secret password to be used in response to an unknown remote peer. You can use any printable characters, including spaces. A password can contain up to 255 printable characters.

Default There is no PPP password defined or configured to a PPP interface by default.

Mode Interface Configuration for a PPP interface

Examples To enable the use of the PPP secret password `bobs_secret` for PPP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp password bobs_secret
```

To disable the use of the PPP secret password `bobs_secret` for PPP authentication, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp password
```

Related commands [ppp authentication](#)
[ppp username](#)

ppp service-name (PPPoE)

Overview This command configures the PPPoE service name used to select a service from an access concentrator. This can only be applied when the PPP interface has been configured over an underlying eth interface.

Use the **no** variant of this command to set the service name for the connection back to the default (unset).

Syntax `ppp service-name <service-name>`
`no ppp service-name`

Parameter	Description
<code><service-name></code>	Specifies the PPPoE service name to select from an access concentrator. The service-name is 1 to 18 characters long, is case-sensitive, and for a PPPoE client is usually supplied by the ISP. The name can contain any printable ASCII characters (ASCII 32-126). If the name contains the special characters backslash, double-quote or space, those characters should be escaped with a backslash. The default is no service name.

Default The default option is not to specify a service name. This results in a connection to the default service specified by the access concentrator.

Mode Interface Configuration for a PPP interface

Usage notes You can only apply a single service name to each PPPoE interface.

Examples To connect to a service called "Internet", use the command:

```
awplus(config)# interface ppp0
awplus(config-if)# ppp service-name Internet
```

Related commands [encapsulation ppp](#)
[show interface \(PPP\)](#)

ppp timeout idle

Overview Use this command to specify an idle time when a PPP connection is disconnected. Use the **no** variant of this command to reset the idle time to the default of 60 seconds.

Syntax `ppp timeout idle <0-99999>`
`no ppp timeout idle`

Parameter	Description
<code><0-99999></code>	The time in seconds before the idle timeout disconnects. If this is not specified the default value of 60 seconds is used.

Default PPP timeout idle is not set and the PPP Dial on Demand feature is disabled. If no idle time is set, the default value of 60 seconds is used.

Mode Interface Configuration

Usage notes This command allows an idle timer to disconnect a PPP connection after a specified time. The timer is reset upon either ingress or regress user traffic. Non-user traffic such as Link Control Protocol (LCP) keepalives and Network Control Protocol (NCP) negotiation packets do not reset the idle timer.

Examples To set the idle time to 30 seconds, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp timeout idle
30
```

To disable the use of the timer and disable the PPP Dial on Demand feature, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp timeout
idle 30
```

Validation Commands `show running-config interface`

ppp username

Overview This command creates or modifies a username for a PPP user on a configured PPP interface.

Syntax `ppp username <username>`
`no ppp username`

Parameter	Description
<code><username></code>	Specify a login name for the user. The name can contain up to 255 characters. The name can contain any printable ASCII characters (ASCII 32-126). If the name contains the special characters backslash, double-quote or space, those characters should be escaped with a backslash.

Default There is no default PPP username defined or configured to a PPP interface.

Mode Interface Configuration for a PPP interface.

Examples To create the PPP username `bob`, for the PPP interface `ppp0`, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp username bob
```

To remove the PPP username `bob`, for the PPP interface `ppp0`, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ppp username
```

Related commands [ppp authentication](#)
[ppp password](#)

show debugging ppp

Overview Use this command to display PPP debug settings for optionally specified PPP interfaces. If no PPP interfaces are specified then PPP debug settings are shown for all available PPP interfaces.

Syntax `show debugging ppp [interface <0-255>]`

Parameter	Description
<0-255>	Specify a PPP interface or a range of PPP interfaces in the range ppp<0-255>. Use a hyphen between PPP interfaces to include all PPP interfaces in a given range, or use commas between PPP interfaces to specify non-contiguous PPP interfaces.

Mode Privileged Exec

Examples The following example shows how to display PPP debug information for PPP interface ppp0:

```
awplus# show debugging ppp interface ppp0
```

The following example shows how to display PPP debug information for PPP interface ppp0 through ppp2:

```
awplus# show debugging ppp interface ppp0-ppp2
```

The following example shows how to display PPP debug information for PPP interface ppp0 and ppp2:

```
awplus# show debugging ppp interface ppp0,ppp2
```

The following example shows how to display PPP debug information for all available PPP interfaces:

```
awplus# show debugging ppp
```

Figure 14-6: Example output from the **show debugging ppp** command

```
awplus# show debugging ppp
PPP debugging status:
  PPP debug on interface ppp0: enabled
  PPP debug on interface ppp1: disabled
```

Related commands

- [debug ppp](#)
- [no debug all](#)
- [undebug all](#)
- [show interface \(PPP\)](#)

show interface (PPP)

Overview Use this command to display configuration and status information for a configured PPP (Point-to-Point) interface.

Syntax `show interface ppp<ppp_index>`

Parameter	Description
<ppp_index>	Display configuration and status information for the specified and configured PPP interface (0 to 255).

Mode User Exec and Privileged Exec

Usage notes See the [show interface brief](#) command for brief interface, configuration and status information.

Note the negotiated options, including those for DNS addresses, are shown in console output:

- Local DNS addresses as displayed in console output are provided from the peer.
- Peer DNS addresses as displayed in console output are provided to the peer.
- Only Peer DNS addresses or Local DNS addresses are shown, but not both.
- Echo Request Timer value as displayed in console output is the local setting.

Example The following example shows how to display the configuration and status information for a configured PPP interface named `ppp0`.

```
awplus# show interface ppp0
```

Figure 14-7: Example output from the **show interface** command for a PPPoE interface

```
awplus#show interface ppp0

Interface ppp0
  Scope: both
  Link is UP, administrative state is UP
  Hardware is PPP
  IPv4 address 10.1.0.2/32
  IPv6 address fe80::200:cdff:fe28:8a1/10
  index 16778440 metric 1
  <UP, POINTOPOINT, RUNNING, NOARP, MULTICAST>
  VRF Binding: Not bound
  PPP is running over interface eth0
  PPPoE is using the default service
  SNMP link-status traps: Disabled
    input packets 12, bytes 458, dropped 0, multicast packets 0
    output packets 6, bytes 122, multicast packets 0 broadcast
    packets 0
  Time since last state change: 0 days 00:01:57
```

Figure 14-8: Example output from the **show interface ppp1** command showing negotiated DNS addresses, where the peer provided the DNS information (see the **Local DNS addresses** field output below):

```
awplus#sh interface ppp1
Interface ppp1
  Scope: both
  Link is UP, administrative state is UP
  Hardware is PPP
  IPv4 address 192.168.1.1/30 pointopoint 192.168.1.2
  IPv6 address fe80::200:cdff:fe28:89f/10
  index 16778241 metric 1 mtu 1460
  <UP, POINTOPOINT, RUNNING, NOARP, MULTICAST>
  VRF Binding: Not bound
  PPP is running over interface tunnel1
  LCP Opened IPCP Opened IPV6CP Opened
  MRU(bytes): Local config 1460, Local negotiated 1460, Peer
negotiated 1460
  Magic number: Local config ON, Local negotiated ON, Peer
negotiated ON
  Authentication: Local config None, Local neg None, Peer neg None
  Echo Request Timer (seconds): 10
  IPv4 addresses: Local config 192.168.1.1, Peer neg 192.168.1.2
  IPv6 interface ID: Local eecd:6dff:fe3a:0d18, Peer neg
eecd:6dff:fe3a:0d18
  Local DNS addresses: 192.168.60.1, 192.168.60.2
  L2TP session ID is 15288
  SNMP link-status traps: Disabled
    input packets 5, bytes 96, dropped 0, multicast packets 0
    output packets 5, bytes 96, multicast packets 0 broadcast
packets 0
  Time since last state change: 0 days 00:06:29
awplus#
```

Figure 14-9: Example output from the **show interface ppp1** command showing negotiated DNS addresses, where the peer was provided with DNS information (see the **Peer DNS addresses** field output below):

```
awplus#sh interface ppp1
Interface ppp1
  Scope: both
  Link is UP, administrative state is UP
  Hardware is PPP
  IPv4 address 192.168.1.1/30 pointopoint 192.168.1.2
  IPv6 address fe80::200:cdff:fe28:89f/10
  index 16778241 metric 1 mtu 1460
  <UP, POINTOPOINT, RUNNING, NOARP, MULTICAST>
  VRF Binding: Not bound
  PPP is running over interface tunnel1
  LCP Opened IPCP Opened IPV6CP Opened
  MRU(bytes): Local config 1460, Local negotiated 1460, Peer
negotiated 1460
  Magic number: Local config ON, Local negotiated ON, Peer
negotiated ON
  Authentication: Local config None, Local neg None, Peer neg None
  Echo Request Timer (seconds): 10
  IPv4 addresses: Local config 192.168.1.1, Peer neg 192.168.1.2
  IPv6 interface ID: Local eecd:6dff:fe3a:0d18, Peer neg
eecd:6dff:fe3a:0d18
  Peer DNS addresses: 1.1.1.1, 2.2.2.2
  L2TP session ID is 15288
  SNMP link-status traps: Disabled
    input packets 5, bytes 96, dropped 0, multicast packets 0
    output packets 5, bytes 96, multicast packets 0 broadcast
packets 0
  Time since last state change: 0 days 00:06:29
awplus#
```

**Related
commands**

[encapsulation ppp](#)
[ppp service-name \(PPPoE\)](#)
[show interface](#)
[show interface brief](#)

undebg ppp

Overview Use this command to disable PPP protocol debugging on the specified PPP interface or interfaces. If no PPP interface is specified then PPP debugging for all PPP interfaces is disabled.

This command has the same functionality as the **no** variant of the [debug ppp](#) command.

Syntax `undebg ppp [interface <ppp-interface-list>]`

Parameter	Description
<ppp-interface-list>	Specify a PPP interface or a range of PPP interfaces in the range ppp<0-255>. Use a hyphen between PPP interfaces to include all PPP interfaces in a given range, or use commas between PPP interfaces to specify non-contiguous PPP interfaces.

Default No diagnostic messages are enabled for PPP debugging. PPP debugging is disabled by default.

Mode Privileged Exec

Usage notes Note that this command is an alias of the negated form of the [debug ppp](#) command.

Examples To disable PPP debugging for all PPP interfaces, enter the below command:

```
awplus# undebg ppp
```

To disable PPP debugging for PPP interfaces ppp0, enter the below command:

```
awplus# undebg ppp interface ppp0
```

To disable PPP debugging for PPP interfaces ppp0 through ppp2, enter the below command:

```
awplus# undebg ppp interface ppp0-ppp2
```

To disable PPP debugging for PPP interfaces ppp0 and ppp2, enter the below command:

```
awplus# undebg ppp interface ppp0,ppp2
```

Related commands

- [debug ppp](#)
- [no debug all](#)
- [show debugging ppp](#)
- [undebg all](#)

15

PPP over Ethernet (PPPoE) Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Point to Point Protocol over Ethernet (PPPoE) related features. This includes PPPoE Client, PPPoE Access Concentrator, and PPPoE Relay.

For more information, see the [PPP Feature Overview and Configuration Guide](#) and the [L2TPv2 Tunneling of PPP Feature Overview and Configuration Guide](#).

- Command List**
- [“client \(pppoe-relay\)”](#) on page 453
 - [“max-sessions”](#) on page 454
 - [“pppoe-relay”](#) on page 455
 - [“server \(pppoe-relay\)”](#) on page 456
 - [“show running-config pppoe-relay”](#) on page 457
 - [“timeout \(pppoe-relay\)”](#) on page 458

client (pppoe-relay)

Overview Use this command to configure a PPPoE relay client interface.
Use the **no** variant of this command to remove a PPPoE relay client interface.

Syntax `client <client-interface>`
`no client <client-interface>`

Parameter	Description
<code><client-interface></code>	The PPPoE relay client interface. The valid interface type is: eth.

Default None.

Mode PPPoE Relay Configuration

Example To configure eth1 as the client interface on PPPoE relay instance 'Telco1', use the commands:

```
awplus# pppoe-relay Telco1
awplus(config-pppoe-relay)# client eth1
```

To remove the eth1 client interface configured on PPPoE relay instance 'Telco1', use the commands:

```
awplus# pppoe-relay Telco1
awplus(config-pppoe-relay)# no client eth1
```

Related commands [server \(pppoe-relay\)](#)
[timeout \(pppoe-relay\)](#)
[max-sessions](#)
[pppoe-relay](#)
[show running-config pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

max-sessions

Overview Use this command to configure the maximum concurrent sessions for a PPPoE relay instance.

Use the **no** variant of this command to set a PPPoE relay maximum concurrent sessions to the default value.

Syntax `max-sessions <1-65534>`
`no max-sessions`

Parameter	Description
<code><1-65534></code>	The maximum number of concurrent sessions per PPPoE relay instance.

Default 5000

Mode PPPoE Relay Configuration

Example To set the PPPoE relay maximum concurrent sessions to 50, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco1
awplus(config-pppoe-relay)# max-sessions 50
```

To set the PPPoE relay maximum concurrent sessions to the default, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco1
awplus(config-pppoe-relay)# no max-sessions
```

Related commands

- [client \(pppoe-relay\)](#)
- [server \(pppoe-relay\)](#)
- [timeout \(pppoe-relay\)](#)
- [pppoe-relay](#)
- [show running-config pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

pppoe-relay

Overview Use this command to create a PPPoE relay instance and put the device into PPPoE Relay Configuration mode, in which subsequent commands can be entered.

Use the **no** variant of this command to remove the PPPoE relay instance and all its configuration.

Syntax `pppoe-relay <relay-name>`
`no pppoe-relay <relay-name>`

Parameter	Description
<code><relay-name></code>	Name of the PPPoE relay instance

Default None.

Mode Global Configuration

Usage notes PPPoE relay tracks state information for multiple Layer 2 PPPoE sessions, and allows multiple PPPoE client connections to be relayed between one or more client LANs and a WAN.

This allows the PPPoE client connections to have access to one or more service provider PPPoE Access Concentrators - whilst at the same time allowing Layer 3 IP traffic routing from the internal LAN(s) to the Internet.

Use this command to first create a PPPoE relay instance, then add a client and server interface to the instance.

Example To configure a PPPoE relay instance, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay test
awplus(config-pppoe-relay)#
```

Related commands [client \(pppoe-relay\)](#)
[server \(pppoe-relay\)](#)
[timeout \(pppoe-relay\)](#)
[max-sessions](#)
[show running-config pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

server (pppoe-relay)

Overview Use this command to configure a PPPoE relay server interface.
Use the **no** variant of this command to remove a PPPoE relay server interface.

Syntax `server <server-interface>`
`no server <server-interface>`

Parameter	Description
<code><server-interface></code>	The PPPoE relay server interface. The valid interface type is: eth.

Default None.

Mode PPPoE Relay Configuration

Example To configure eth1 as the server interface on PPPoE relay instance 'Telco2', use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco2
awplus(config-pppoe-relay)# server eth1
```

To remove the eth1 server interface configured on PPPoE relay instance 'Telco2', use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco2
awplus(config-pppoe-relay)# no server eth1
```

Related commands [client \(pppoe-relay\)](#)
[timeout \(pppoe-relay\)](#)
[max-sessions](#)
[pppoe-relay](#)
[show running-config pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

show running-config pppoe-relay

Overview Use this command to display the running configuration for PPPoE relay.

Syntax `show running-config pppoe-relay [<relay-name>]`

Parameter	Description
<code><relay-name></code>	Name of the PPPoE relay instance.

Default None.

Mode Privileged Exec

Example To show all PPPoE relay configurations, use the command:

```
awplus# show running-config pppoe-relay
```

To show the PPPoE relay configuration for Telco1, use the command:

```
awplus# show running-config pppoe-relay Telco1
```

Output Figure 15-1: Example output from **show running-config pppoe-relay**

```
awplus#show running-config pppoe-relay
pppoe-relay Telco1
  client eth2
  server vlan4
  max-sessions 50
  timeout 100
!
pppoe-relay Telco2
  client eth1
  server vlan1
!
```

Related commands

- [client \(pppoe-relay\)](#)
- [server \(pppoe-relay\)](#)
- [timeout \(pppoe-relay\)](#)
- [max-sessions](#)
- [pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

timeout (pppoe-relay)

Overview Use this command to configure the PPPoE relay idle session timeout.

Use the **no** variant of this command to set the PPPoE relay idle session timeout to the default value.

Syntax `timeout {0|<30-86400>}`
`no timeout`

Parameter	Description
0	Sets the idle session timeout to never terminate PPPoE relay sessions.
<30-86400>	The PPPoE relay idle session timeout in seconds.

Default 600 seconds.

Mode PPPoE Relay Configuration

Example To set the PPPoE relay idle session timeout to 30 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco1
awplus(config-pppoe-relay)# timeout 1800
```

To set the PPPoE relay idle session timeout to never timeout, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco1
awplus(config-pppoe-relay)# timeout 0
```

To set the PPPoE relay idle session timeout to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# pppoe-relay Telco1
awplus(config-pppoe-relay)# no timeout
```

Related commands

- [client \(pppoe-relay\)](#)
- [server \(pppoe-relay\)](#)
- [max-sessions](#)
- [pppoe-relay](#)
- [show running-config pppoe-relay](#)

Command changes Version 5.5.0-1.3: command added

Part 3: Routing

16

IP Addressing and Protocol Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure various IP features, including the following protocols:

- Address Resolution Protocol (ARP)

For more information, see the [IP Feature Overview and Configuration Guide](#).

- Command List**
- [“arp”](#) on page 462
 - [“arp log”](#) on page 463
 - [“arp opportunistic-nd”](#) on page 466
 - [“arp-loose-check”](#) on page 467
 - [“arp-reply-bc-dmac”](#) on page 469
 - [“clear arp-cache”](#) on page 470
 - [“debug ip packet interface”](#) on page 471
 - [“ip address \(IP Addressing and Protocol\)”](#) on page 473
 - [“ip directed-broadcast”](#) on page 475
 - [“ip forwarding”](#) on page 477
 - [“ip forward-protocol udp”](#) on page 478
 - [“ip helper-address”](#) on page 480
 - [“ip icmp error-interval”](#) on page 482
 - [“ip icmp-timestamp”](#) on page 483
 - [“ip limited-local-proxy-arp”](#) on page 484
 - [“ip local-proxy-arp”](#) on page 485
 - [“ip proxy-arp”](#) on page 486
 - [“ip redirects”](#) on page 487

- ["ip tcp synack-retries"](#) on page 488
- ["ip tcp timeout established"](#) on page 489
- ["ip tcp-timestamp"](#) on page 490
- ["ip unreachable"](#) on page 491
- ["local-proxy-arp"](#) on page 493
- ["ping"](#) on page 494
- ["show arp"](#) on page 495
- ["show debugging ip packet"](#) on page 497
- ["show ip flooding-nexthops"](#) on page 498
- ["show ip forwarding"](#) on page 499
- ["show ip interface"](#) on page 500
- ["show ip sockets"](#) on page 501
- ["show ip traffic"](#) on page 504
- ["tcpdump"](#) on page 506
- ["traceroute"](#) on page 507
- ["undebg ip packet interface"](#) on page 508

arp

Overview This command adds a static ARP entry to the ARP cache. This is typically used to add entries for hosts that do not support ARP or to speed up the address resolution function for a host. The ARP entry must not already exist. Use the **alias** parameter to allow your device to respond to ARP requests for this IP address.

The **no** variant of this command removes the static ARP entry. Use the [clear arp-cache](#) command to remove the dynamic ARP entries in the ARP cache.

Syntax `arp <ip-addr> <mac-address> [alias]`
`no arp <ip-addr>`

Parameter	Description
<code><ip-addr></code>	The IPv4 address of the device you are adding as a static ARP entry.
<code><mac-address></code>	The MAC address of the device you are adding as a static ARP entry, in hexadecimal notation with the format HHHH.HHHH.HHHH.
<code>alias</code>	Allows your device to respond to ARP requests for the IP address. Proxy ARP must be enabled on the interface before using this parameter.

Mode Global Configuration

Examples To add the IP address 10.10.10.9 with the MAC address 0010.2533.4566 into the ARP cache, and have your device respond to ARP requests for this address, use the commands:

```
awplus# configure terminal
awplus(config)# arp 10.10.10.9 0010.2533.4566 alias
```

Related commands [clear arp-cache](#)
[ip proxy-arp](#)
[show arp](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

arp log

Overview This command enables the logging of dynamic and static ARP entries in the ARP cache. The ARP cache contains mappings of IP addresses to physical MAC addresses for hosts.

This command can display the MAC addresses in the ARP log either using the notation HHHH.HHHH.HHHH, or using the IEEE standard hexadecimal notation (HH-HH-HH-HH-HH-HH).

Use the **no** variant of this command to disable the logging of ARP entries.

Syntax `arp log [mac-address-format ieee]`
`no arp log [mac-address-format ieee]`

Parameter	Description
<code>mac-address-format ieee</code>	Display the MAC address in the standard IEEE format (HH-HH-HH-HH-HH-HH), instead of displaying the MAC address with the format HHHH.HHHH.HHHH.

Default The ARP logging feature is disabled by default.

Mode Global Configuration

Usage notes You have the option to change how the MAC address is displayed in the ARP log message. The output can either use the notation HHHH.HHHH.HHHH or HH-HH-HH-HH-HH-HH.

Enter **arp log** to use HHHH.HHHH.HHHH notation.

Enter **arp log mac-address-format ieee** to use HH-HH-HH-HH-HH-HH notation.

Enter **no arp log mac-address-format ieee** to revert from HH-HH-HH-HH-HH-HH to HHHH.HHHH.HHHH.

Enter **no arp log** to disable ARP logging.

To display ARP log messages use the command **show log | include ARP_LOG**.

Examples To enable ARP logging and specify that the MAC address in the log message is displayed in HHHH.HHHH.HHHH notation, use the following commands:

```
awplus# configure terminal
awplus(config)# arp log
```

To disable ARP logging on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log
```

To enable ARP logging and specify that the MAC address in the log message is displayed in the standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH), use the following commands:

```
awplus# configure terminal
awplus(config)# arp log mac-address-format ieee
```

To leave ARP logging enabled, but stop using HH-HH-HH-HH-HH-HH format and use HHHH.HHHH.HHHH format instead, use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log mac-address-format ieee
```

To display ARP log messages, use the following command:

```
awplus# show log | include ARP_LOG
```

Output Figure 16-1: Output from **show log | include ARP_LOG** after enabling ARP logging using **arp log**. Note that this output uses HHHH.HHHH.HHHH format.

```
awplus#configure terminal
awplus(config)#arp log
awplus(config)#exit
awplus#show log | include ARP_LOG
2022 Mar 6 06:21:01 user.notice awplus HSL[1007]: ARP_LOG eth1 add
0013.4078.3b98 (192.168.2.4)
2022 Mar 6 06:22:30 user.notice awplus HSL[1007]: ARP_LOG eth1 del
0013.4078.3b98 (192.168.2.4)
2022 Mar 6 06:23:26 user.notice awplus HSL[1007]: ARP_LOG eth1 add
0030.940e.136b (192.168.2.20)
2022 Mar 6 06:23:30 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Figure 16-2: Output from **show log | include ARP_LOG** after enabling ARP logging using **arp log mac-address format ieee**. Note that this output uses HH-HH-HH-HH-HH-HH format.

```
awplus#configure terminal
awplus(config)#arp log mac-address-format ieee
awplus(config)#exit
awplus#show log | include ARP_LOG
2022 Mar 6 06:25:28 user.notice awplus HSL[1007]: ARP_LOG eth1 add 00-17-9a-b6-03-69
(192.168.2.12)
2022 Mar 6 06:25:30 user.notice awplus HSL[1007]: ARP_LOG eth1 add 00-03-37-6b-a6-a5
(192.168.2.10)
2022 Mar 6 06:26:53 user.notice awplus HSL[1007]: ARP_LOG eth1 del 00-30-94-0e-13-6b
(192.168.2.20)
2022 Mar 6 06:27:31 user.notice awplus HSL[1007]: ARP_LOG eth1 del 00-17-9a-b6-03-69
(192.168.2.12)
2022 Mar 6 06:28:09 user.notice awplus HSL[1007]: ARP_LOG eth1 del 00-03-37-6b-a6-a5
(192.168.2.10)
2022 Mar 6 06:28:14 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

The following table lists the parameters shown in the output of the **show log | include ARP_LOG** command. The ARP log message format is:

```
<date> <time> <severity> <hostname> <program-name>  
ARP_LOG <port-number> <vid> <operation> <MAC> <IP>
```

Table 16-1: Parameters in the output from **show log | include ARP_LOG**

Parameter	Description
ARP_LOG	Indicates that ARP log entry information follows.
<operation>	Indicates "add" if the ARP log entry displays an ARP addition. Indicates "del" if the ARP log entry displays an ARP deletion.
<MAC>	Indicates the MAC address for the ARP log entry, either in the default hexadecimal notation (HHHH.HHHH.HHHH) or in the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) as specified with the arp log or the arp log mac-address-format ieee command.
<IP>	Indicates the IP address for the ARP log entry.

Related commands [show log](#)
[show running-config](#)

arp opportunistic-nd

Overview Use this command to enable opportunistic neighbor discovery for the global ARP cache. This command changes the behavior for unsolicited ARP packet forwarding on the device.

CAUTION: *Opportunistic neighbor discovery can make your device more vulnerable to ARP/ND cache poisoning attacks. We recommend disabling it unless necessary.*

Use the **no** variant of this command to disable opportunistic neighbor discovery for the global ARP cache.

Syntax `arp opportunistic-nd`
`no arp opportunistic-nd`

Default Opportunistic neighbor discovery is disabled by default.

Mode Global Configuration

Usage notes When opportunistic neighbor discovery is enabled, the device will reply to any received unsolicited ARP packets (but not gratuitous ARP packets). The source MAC address for the unsolicited ARP packet is added to the ARP cache, so the device forwards the ARP packet. When opportunistic neighbor discovery is disabled, the source MAC address for the ARP packet is not added to the ARP cache, so the ARP packet is not forwarded by the device.

Examples To enable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# arp opportunistic-nd
```

To disable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# no arp opportunistic-nd
```

Related commands [ipv6 opportunistic-nd](#)
[show arp](#)
[show running-config interface](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

arp-loose-check

Overview Use this command to let AlliedWare Plus process ARPs that have a sender protocol address from outside the interface's local subnets.

Use the **no** variant of this command to return to the default ARP processing behavior. By default, AlliedWare Plus will only process ARP packets that are local to the incoming interface.

Syntax `arp-loose-check`
`no arp-loose-check`

Default Disabled.

Mode Interface Configuration for Eth, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

Usage notes By default, AlliedWare Plus will only process ARP packets that are local to the incoming interface, to prevent ARP poisoning. This means the packets must have:

- a sender protocol address inside one of the incoming interface's local subnets, and
- a target protocol address equal to one of the incoming interface's IP addresses.

If you enable loose ARP processing and then use the **no** variant of this command to return to default processing, you may need to clear the ARP cache. Use the [clear arp-cache](#) command. This will remove any undesired existing ARPs.

You cannot use this command at the same time as Proxy ARP. Proxy ARP also allows AlliedWare Plus to process ARPs that have a sender protocol address from outside the interface's local subnets.

Example To process ARPs that have a sender protocol address from outside eth1's local subnets, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# arp-loose-check
```

To return to the default behavior on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no arp-loose-check
```

Related commands [arp](#)
[clear arp-cache](#)
[ip proxy-arp](#)
[show arp](#)

Command changes Version 5.5.2-0.1: command added

arp-reply-bc-dmac

Overview Use this command to allow processing of ARP replies that arrive with a broadcast destination MAC (ffff.ffff.ffff). This makes neighbors reachable if they send ARP responses that contain a broadcast destination MAC.

Use the **no** variant of this command to turn off processing of ARP replies that arrive with a broadcast destination MAC.

Syntax `arp-reply-bc-dmac`
`no arp-reply-bc-dmac`

Default By default, this functionality is disabled.

Mode Interface Configuration for Eth, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

Example To allow processing of ARP replies that arrive on eth0 with a broadcast destination MAC, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# arp-reply-bc-dmac
```

Related commands [clear arp-cache](#)
[show arp](#)

clear arp-cache

Overview This command deletes dynamic ARP entries from the ARP cache. You can optionally specify the IPv4 address of an ARP entry to be cleared from the ARP cache.

Syntax `clear arp-cache [<ip-address>]`

Parameter	Description
<code><ip-address></code>	The IPv4 address of an ARP entry that is to be cleared from the ARP cache.

Mode Privileged Exec

Usage notes To display the entries in the ARP cache, use the [show arp](#) command. To remove static ARP entries, use the no variant of the [arp](#) command.

Example To clear all dynamic ARP entries, use the command:

```
awplus# clear arp-cache
```

To clear all dynamic ARP entries associated with the IPv4 address 192.168.1.1, use the command:

```
awplus# clear arp-cache 192.168.1.1
```

Related commands [arp](#)
[show arp](#)

debug ip packet interface

- Overview** The **debug ip packet interface** command enables IP packet debug and is controlled by the **terminal monitor** command.
- If the optional **icmp** keyword is specified then ICMP packets are shown in the output.
- The **no** variant of this command disables the **debug ip packet interface** command.

Syntax `debug ip packet interface {<interface-name>|all} [address <ip-address>|verbose|hex|arp|udp|tcp|icmp]`

`no debug ip packet interface [<interface-name>]`

Parameter	Description
<interface-name>	Specify a single Layer 3 interface name (not a range of interfaces) This keyword can be specified as either all or as a single Layer 3 interface to show debugging for either all interfaces or a single interface.
all	Specify all Layer 3 interfaces on the device.
<ip-address>	Specify an IPv4 address. If this keyword is specified, then only packets with the specified IP address as specified in the ip-address placeholder are shown in the output.
verbose	Specify verbose to output more of the IP packet. If this keyword is specified then more of the packet is shown in the output.
hex	Specify hex to output the IP packet in hexadecimal. If this keyword is specified, then the output for the packet is shown in hex.
arp	Specify arp to output ARP protocol packets. If this keyword is specified, then ARP packets are shown in the output.
udp	Specify udp to output UDP protocol packets. If this keyword is specified then UDP packets are shown in the output.
tcp	Specify tcp to output TCP protocol packets. If this keyword is specified, then TCP packets are shown in the output.
icmp	Specify icmp to output ICMP protocol packets. If this keyword is specified, then ICMP packets are shown in the output.

Mode Privileged Exec and Global Configuration

Examples To turn on ARP packet debugging on eth0, use the command:

```
awplus# debug ip packet interface eth0 arp
```

To turn off IP packet interface debugging on interface eth0, use the command:

```
awplus# no debug ip packet interface eth0
```

To turn on all packet debugging on all interfaces on the device, use the command:

```
awplus# debug ip packet interface all
```

To turn off IP packet interface debugging on all interfaces, use the command:

```
awplus# no debug ip packet interface
```

To turn on TCP packet debugging on eth0 and IP address 192.168.2.4, use the command:

```
awplus# debug ip packet interface eth0 address 192.168.2.4 tcp
```

Related commands

- [no debug all](#)
- [show debugging ip dns forwarding](#)
- [tcpdump](#)
- [terminal monitor](#)
- [undebug ip packet interface](#)

ip address (IP Addressing and Protocol)

Overview This command sets a static IP address on an interface.

The **no** variant of this command removes the IP address from the interface.

You cannot remove the primary address when a secondary address is present.

Syntax `ip address <ip-addr/prefix-length> [secondary] [label <label>]`
`no ip address [<ip-addr/prefix-length>] [secondary]`

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length you are assigning to the interface.
secondary	Secondary IP address.
label	Adds a user-defined description of the secondary IP address.
<label>	A user-defined description of the secondary IP address. Valid characters are any printable character and spaces.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes To set the primary IP address on the interface, specify only **ip address** <ip-addr/prefix-length>. This overwrites any configured primary IP address. To add additional IP addresses on this interface, use the **secondary** parameter. You must configure a primary address on the interface before configuring a secondary address.

NOTE: Use **show running-config interface**, instead of **show ip interface brief**, when you need to view a secondary address configured on an interface. **show ip interface brief** will only show the primary address, not a secondary address for an interface.

Examples To add the IP address 10.10.10.50/24 to the interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip address 10.10.10.50/24
```

To add the secondary IP address 10.10.11.50/24 to the same interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip address 10.10.11.50/24 secondary
```

To add the IP address 10.10.11.50/24 to the local loopback interface lo, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the tunnel tunnel0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# ip address 10.10.11.50/24
```

**Related
commands**

[interface \(to configure\)](#)
[show ip interface](#)
[show running-config interface](#)

ip directed-broadcast

Overview Use this command to enable flooding of directed broadcast packets into a directly connected subnet. If this command is configured on an interface, then directed broadcasts received on other interfaces, destined for the subnet on this interface, will be flooded to the subnet broadcast address of this interface.

Use the **no** variant of this command to disable **ip directed-broadcast**. When this feature is disabled using the **no** variant of this command, directed broadcasts are not forwarded.

Syntax `ip directed-broadcast`
`no ip directed-broadcast`

Default The **ip directed-broadcast** command is disabled by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes IP directed-broadcast is enabled and disabled per interface. When enabled a directed broadcast packet is forwarded to an enabled interface if received on another subnet.

An IP directed broadcast is an IP packet whose destination address is a broadcast address for some IP subnet, but originates from a node that is not itself part of that destination subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is flooded as a broadcast on the destination subnet.

The **ip directed-broadcast** command controls the flooding of directed broadcasts when they reach target subnets. The command affects the final transmission of the directed broadcast on its destination subnet. It does not affect the transit unicast routing of IP directed broadcasts. If directed broadcast is enabled for an interface, incoming directed broadcast IP packets intended for the subnet assigned to the interface will be flooded as broadcasts on that subnet.

If the **no ip directed-broadcast** command is configured for an interface, directed broadcasts destined for the subnet where the interface is attached will be dropped instead of broadcast.

Examples To enable the flooding of broadcast packets via the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip directed-broadcast
```

To disable the flooding of broadcast packets via the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip directed-broadcast
```

Related commands

- [ip forward-protocol udp](#)
- [ip helper-address](#)
- [show running-config](#)

ip forwarding

Overview This command enables IP forwarding on your device. When enabled, your device routes IP packets.

The **no** variant of this command disables IP forwarding on your device. Even when IP forwarding is not enabled, the device can still work as an IP host; in particular, it can be managed by IP-based applications, such as SNMP, Telnet and SSH.

Syntax `ip forwarding`
`no ip forwarding`

Default IP forwarding is enabled by default.

Mode Global Configuration

Examples To enable your device to route IP packets, use the commands:

```
awplus# configure terminal
awplus(config)# ip forwarding
```

To stop your device from routing IP packets, use the commands

```
awplus# configure terminal
awplus(config)# no ip forwarding
```

Related commands [show ip forwarding](#)

ip forward-protocol udp

Overview This command enables you to control which UDP broadcasts will be forwarded to the helper address(es). A UDP broadcast will only be forwarded if the destination UDP port number in the packet matches one of the port numbers specified using this command.

Refer to the IANA site (www.iana.org) for a list of assigned UDP port numbers for protocols to forward using **ip forward-protocol udp**.

Use the **no** variant of this command to remove a port number from the list of destination port numbers that are used as the criterion for deciding if a given UDP broadcast should be forwarded to the IP helper address(es).

Syntax `ip forward-protocol udp <port>`
`no ip forward-protocol udp <port>`

Parameter	Description
<port>	UDP Port Number.

Default The **ip forward-protocol udp** command is not enabled by default.

Mode Global Configuration

Usage notes Combined with the **ip helper-address** command in interface mode, the **ip forward-protocol udp** command in Global Configuration mode allows control of which protocols (destination port numbers) are forwarded. The **ip forward-protocol udp** command configures protocols for forwarding, and the **ip helper-address** command configures the destination address(es).

NOTE:

*The types of UDP broadcast packets that the device will forward are ONLY those specified by the **ip forward-protocol** command(s). There are no other UDP packet types that the IP helper process forwards by default.*

Examples To configure forwarding of packets on a UDP port, use the following commands:

```
awplus# configure terminal
awplus(config)# ip forward-protocol udp <port>
```

To delete a UDP port from the UDP ports that the device forwards, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip forward-protocol udp <port>
```

**Related
commands**

- [ip helper-address](#)
- [ip directed-broadcast](#)
- [show running-config](#)

ip helper-address

Overview Use this command to add a forwarding destination address for IP Helper to enable forwarding of User Datagram Protocol (UDP) broadcasts on an interface.

Use the **no** variant of this command to disable the forwarding of broadcast packets to specific addresses.

Syntax `ip helper-address <ip-addr>`
`no ip helper-address <ip-addr>`

Parameter	Description
<ip-addr>	Forwarding destination IP address for IP Helper.

Default The destination address for the **ip helper-address** command is not configured by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes Combined with the [ip forward-protocol udp](#) command in global configuration mode, the **ip helper-address** command in interface mode allows control of which protocols (destination port numbers) are forwarded. The **ip forward-protocol udp** command configures protocols for forwarding, and the **ip helper-address** command configures the destination address(es).

The destination address can be a unicast address or a subnet broadcast address. The UDP destination port is configured separately with the **ip forward-protocol udp** command. If multiple destination addresses are registered then UDP packets are forwarded to each IP address added to an IP Helper. Up to 32 destination addresses may be added using IP Helper.

The device will only forward the types of UDP broadcast packets that are specified by the **ip forward-protocol** command(s). The device does not forward any other UDP packet types by default.

The **ip helper-address** command does not support BOOTP / DHCP Relay. The [service dhcp-relay](#) command must be used instead. For this reason, you may not configure UDP ports 67 and 68 with the **ip forward-protocol** command.

See the [IP Feature Overview and Configuration Guide](#) for more information about DHCP Relay.

Examples The following example defines IPv4 address 192.168.1.100 as an IP Helper destination address to which to forward UDP broadcasts received on eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip helper-address 192.168.1.100
```

The following example removes IPv4 address 192.168.1.100 as an IP Helper destination address to which to forward UDP broadcasts received on eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip helper-address 192.168.1.100
```

Related commands

- [ip forward-protocol udp](#)
- [ip directed-broadcast](#)
- [show running-config](#)

ip icmp error-interval

Overview Use this command to limit how often IPv4 ICMP error messages are sent. The maximum frequency of messages is specified in milliseconds.

Use the **no** variant of this command to reset the frequency to the default.

Syntax `ip icmp error-interval <interval>`
`no ip icmp error-interval`

Parameter	Description
<interval>	0-2147483647, interval in milliseconds.

Default 1000

Mode Global Configuration

Example To configure the rate to be at most one packet every 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip icmp error-interval 10000
```

To reset the rate to the default of one packet every second, use the commands:

```
awplus# configure terminal
awplus(config)# no ip icmp error-interval
```

Related commands [ipv6 icmp error-interval](#)

ip icmp-timestamp

Overview Use this command to allow ICMP timestamp request and response packets.

Use the **no** variant of this command to drop ICMP timestamp request and response packets.

You may wish to drop these packets because the ICMP timestamp response contains the device's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services. In addition, it may be possible to fingerprint devices by analyzing their responses to invalid ICMP timestamp requests.

Syntax `ip icmp-timestamp`
`no ip icmp-timestamp`

Default Allowed

Mode Global Configuration

Example To drop ICMP timestamp packets, use the commands:

```
awplus# configure terminal
awplus(config)# no ip icmp-timestamp
```

To allow ICMP timestamp packets again, use the commands:

```
awplus# configure terminal
awplus(config)# ip icmp-timestamp
```

Related commands [ip tcp-timestamp](#)

Command changes Version 5.5.2-0.1: command added

ip limited-local-proxy-arp

Overview Use this command to enable local proxy ARP, but only for a specified set of IP addresses. This makes the device respond to ARP requests for those IP addresses when the addresses are reachable via the interface you are configuring.

To specify the IP addresses, use the command [local-proxy-arp](#).

Use the **no** variant of this command to disable limited local proxy ARP. This stops your device from intercepting and responding to ARP requests for the specified hosts. This allows the hosts to use MAC address resolution to communicate directly with one another.

Syntax `ip limited-local-proxy-arp`
`no ip limited-local-proxy-arp`

Default Limited local proxy ARP is disabled by default.

Mode Interface Configuration for Eth, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

Usage Limited local proxy ARP supports Static NAT configurations in which the NAT configuration's public address is different to the Ethernet interface's address.

On such Ethernet interfaces, the device needs to respond to ARP requests for the public address so that it will receive packets targeted at that address.

Limited local proxy ARP makes this possible. It is especially useful when you have a number of 1-1 NAT configurations and each public address falls within the public interface's subnet. If you enable limited local proxy ARP on the public interface and specify suitable addresses, the device will respond to ARP requests for those addresses, as long as the addresses are routed out the interface the ARP requests are received on. The device responds with its own MAC address.

Related commands [ip local-proxy-arp](#)
[local-proxy-arp](#)

ip local-proxy-arp

Overview This command allows you to stop MAC address resolution between hosts within a subnet. Local Proxy ARP works by intercepting ARP requests between hosts within a subnet and responding with your device's own MAC address details instead of the destination host's details. This stops hosts from learning the MAC address of other hosts within its subnet through ARP requests.

Local Proxy ARP ensures that devices within a subnet cannot send traffic that bypasses Layer 3 routing on your device. This lets you monitor and filter traffic between hosts in the same subnet, and enables you to have control over which hosts may communicate with one another.

When Local Proxy ARP is operating on an interface, your device does not generate or forward any ICMP-Redirect messages on that interface. This command does not enable proxy ARP on the interface; see the [ip proxy-arp](#) command for more information on enabling proxy ARP.

The **no** variant of this command disables Local Proxy ARP to stop your device from intercepting and responding to ARP requests between hosts within a subnet. This allows the hosts to use MAC address resolution to communicate directly with one another. Local Proxy ARP is disabled by default.

Syntax `ip local-proxy-arp`
`no ip local-proxy-arp`

Default Local Proxy ARP is disabled by default.

Mode Interface Configuration for Eth, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

Examples To enable your device to apply Local Proxy ARP on the interface eth1.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
awplus(config-if)# ip local-proxy-arp
```

To stop your device from doing Local Proxy ARP on the interface eth1.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
awplus(config-if)# no ip local-proxy-arp
```

Related commands [ip proxy-arp](#)
[show arp](#)
[show running-config](#)

ip proxy-arp

Overview This command enables Proxy ARP responses to ARP requests on an interface. When enabled, your device intercepts ARP broadcast packets and substitutes its own physical address for that of the remote host. By responding to the ARP request, your device ensures that subsequent packets from the local host are directed to its physical address, and it can then forward these to the remote host.

Your device responds only when it has a specific route to the address being requested, excluding the interface route that the ARP request arrived from. It ignores all other ARP requests. See the [ip local-proxy-arp](#) command about enabling your device to respond to other ARP messages.

The **no** variant of this command disables Proxy ARP responses on an interface. Proxy ARP is disabled by default.

Syntax `ip proxy-arp`
`no ip proxy-arp`

Default Proxy ARP is disabled by default.

Mode Interface Configuration for Eth, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

Examples To enable your device to do Proxy ARP on the interface eth1.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
awplus(config-if)# ip proxy-arp
```

To stop your device from doing Proxy ARP on the interface eth1.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
awplus(config-if)# no ip proxy-arp
```

Related commands [arp](#)
[ip local-proxy-arp](#)
[show arp](#)
[show running-config](#)

ip redirects

Overview This command enables the device to send ICMP redirects.

Use the **no** variant of this command to stop the device from sending ICMP redirects.

Syntax `ip redirects`
`no ip redirects`

Default ICMP redirects are disabled by default.

Mode Global Configuration.

Usage notes ICMP redirect messages are used to notify hosts that a better route is available to a destination.

ICMP redirects are used when a packet is routed into the device on the same interface that the packet is routed out of the device. ICMP redirects are only sent to packet sources that are directly connected to the device.

Examples To enable the switch to send ICMP redirects, use the following commands:

```
awplus# configure terminal
awplus(config)# ip redirects
```

To stop the switch from sending ICMP redirects, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip redirects
```

ip tcp synack-retries

Overview Use this command to specify how many times the switch will retry sending a SYN ACK for a TCP connection for which it has received a SYN but not an ACK. Such connections are called half-open TCP connections. This command allows you to influence how long half-open TCP connections take to time out.

Use the **no** variant of this command to return to the default setting of 5 retries.

Syntax `ip tcp synack-retries <0-255>`
`no ip tcp synack-retries`

Parameter	Description
<0-255>	Number of times to retry sending the SYN ACK

Default 5 retries

Mode Global Configuration

Usage notes The following table shows the approximate correlation between the number of retries and the time half-open TCP connections take to time out.

Number of retries	Approximate lower bound for the timeout
0 retries	1 second
1 retry	3 seconds
2 retries	7 seconds
3 retries	15 seconds
4 retries	31 seconds
5 retries	63 seconds

Example To retry twice, which leads to a timeout of approximately 7 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip tcp synack-retries 2
```

Related commands [show running-config](#)

Command changes Version 5.4.7-0.2: command added

ip tcp timeout established

Overview Use this command to set the idle timeout for all established TCP connections.

Use the **no** variant of this command to set the idle timeout back to the default of 3600 seconds.

Syntax `ip tcp timeout established <1-31536000>`
`no ip tcp timeout established`

Parameter	Description
<code><1-31536000></code>	Idle timeout for established TCP connections in seconds from 1 to 3153600.

Default 3600 seconds (1 hour)

Mode Global Configuration

Usage notes By default, when a TCP session is successfully established through the firewall, when the session goes idle, it automatically times out of the firewall connection tracking table after 3600 seconds. In some situations it may be beneficial to time out unused established TCP sessions earlier.

For example, in a busy environment where there is an excessive number of sessions being established, the firewall connection tracking table could become oversubscribed, with new connections being blocked until older sessions are timed out.

Example To set a non-default TCP session timeout for established idle sessions of 1800 seconds (30 minutes), use the commands:

```
awplus# configure terminal
awplus(config)# ip tcp timeout established 1800
```

Example To set the TCP session timeout for established idle sessions back to the default setting of 3600 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip tcp timeout established
```

Related commands [show running-config](#)

Command changes Version 5.4.6-1.1: command added

ip tcp-timestamp

Overview Use this command to enable TCP timestamp responses.

Use the **no** variant of this command to disable TCP timestamp responses.

You may wish to disable timestamp responses because TCP timestamps may allow other parties to remotely calculate the system uptime and boot time of the device and the device's clock. To prevent this information leaking to potential attackers, we recommend you disable TCP timestamps on the device, unless you need to use them.

Syntax `ip tcp-timestamp`
`no ip tcp-timestamp`

Default Enabled

Mode Global Configuration

Example To disable TCP timestamp responses, use the commands:

```
awplus# configure terminal
awplus(config)# no ip tcp-timestamp
```

To enable TCP timestamp responses again, use the commands:

```
awplus# configure terminal
awplus(config)# ip tcp-timestamp
```

Related commands [ip icmp-timestamp](#)

Command changes Version 5.5.2-0.1: command added

ip unreachables

Overview Use this command to enable ICMP (Internet Control Message Protocol) type 3, destination unreachable, messages.

Use the **no** variant of this command to disable destination unreachable messages. This prevents an attacker from using these messages to discover the topology of a network.

Syntax `ip unreachables`
`no ip unreachables`

Default Destination unreachable messages are enabled by default.

Mode Global Configuration

Usage notes When a device receives a packet for a destination that is unreachable it returns an ICMP type 3 message, this message includes a reason code, as per the table below. An attacker can use these messages to obtain information regarding the topology of a network. Disabling destination unreachable messages, using the **no ip unreachables** command, secures your network against this type of probing.

NOTE: *Disabling ICMP destination unreachable messages breaks applications such as traceroute and Path MTU Discovery (PMTUD), which depend on these messages to operate correctly.*

Table 16-2: ICMP type 3 reason codes and description

Code	Description [RFC]
0	Network unreachable [RFC792]
1	Host unreachable [RFC792]
2	Protocol unreachable [RFC792]
3	Port unreachable [RFC792]
4	Fragmentation required, and DF flag set [RFC792]
5	Source route failed [RFC792]
6	Destination network unknown [RFC1122]
7	Destination host unknown [RFC1122]
8	Source host isolated [RFC1122]
9	Network administratively prohibited [RFC768]
10	Host administratively prohibited [RFC869]
11	Network unreachable for Type of Service [RFC908]
12	Host unreachable for Type of Service [RFC938]
13	Communication administratively prohibited [RFC905]

Table 16-2: ICMP type 3 reason codes and description (cont.)

Code	Description [RFC]
14	Host Precedence Violation [RFC1812]
15	Precedence cutoff in effect [RFC1812]

Example To disable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# no ip unreachable
```

To enable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# ip unreachable
```


local-proxy-arp

Overview Use this command to specify an IP subnet for use with limited local proxy ARP. When limited local proxy ARP is enabled with the command [ip limited-local-proxy-arp](#), the device will respond to ARP requests for addresses in that subnet.

Use the **no** variant of this command to stop specifying a subnet for use with limited local proxy ARP.

Syntax `local-proxy-arp [<ip-add/mask>]`
`no local-proxy-arp [<ip-add/mask>]`

Parameter	Description
<code><ip-add/mask></code>	The IP subnet to use with limited local proxy ARP, in dotted decimal format (A.B.C.D/M). To specify a single IP address, use a 32-bit mask.

Default No subnets are specified for use with limited local proxy ARP.

Mode Global Configuration

Example To specify limited local proxy ARP for the address 172.22.0.3, use the following commands:

```
awplus# configure terminal
awplus(config)# local-proxy-arp 172.22.0.3/32
```

This is part of a configuration snippet that shows how to use limited local proxy ARP with static NAT. See the command [ip limited-local-proxy-arp](#) for the whole example.

Related commands [ip limited-local-proxy-arp](#)

ping

Overview This command sends a query to another IPv4 host (send Echo Request messages).

Syntax ping [ip] <host> [broadcast] [df-bit {yes|no}] [interval <0-128>] [pattern <hex-data-pattern>] [repeat {<1-2147483647>|continuous}] [size <36-18024>] [source <ip-addr>] [timeout <1-65535>] [tos <0-255>]

Parameter	Description
<host>	The destination IP address or hostname.
broadcast	Allow pinging of a broadcast address.
df-bit	Enable or disable the do-not-fragment bit in the IP header.
interval <0-128>	Specify the time interval in seconds between sending ping packets. The default is 1. You can use decimal places to specify fractions of a second. For example, to ping every millisecond, set the interval to 0.001.
pattern <hex-data-pattern>	Specify the hex data pattern.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
continuous	Continuous ping
size <36-18024>	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
source <ip-addr>	The IP address of a configured IP interface to use as the source in the IP header of the ping packet.
timeout <1-65535>	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.
tos <0-255>	The value of the type of service in the IP header.

Mode User Exec and Privileged Exec

Example To ping the IP address 10.10.0.5 use the following command:

```
awplus# ping 10.10.0.5
```

Command changes Version 5.4.6-2.1: VRF-lite support added.

show arp

Overview Use this command to display entries in the ARP routing and forwarding table—the ARP cache contains mappings of IP addresses to physical addresses for hosts. To have a dynamic entry in the ARP cache, a host must have used the ARP protocol to access another host.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show arp`

Mode User Exec and Privileged Exec

Usage notes Running this command with no additional parameters will display all entries in the ARP routing and forwarding table.

Example To display all ARP entries in the ARP cache, use the following command:

```
awplus# show arp
```

Output Figure 16-3: Example output from the **show arp** command

awplus#show arp					
IP Address	LL Address	Interface	Port	Type	
192.168.3.2	0000.cd37.04de	eth0.3	–	dynamic	
10.34.180.4	0800.278c.aaba	eth0.1034	–	dynamic	
10.34.180.254	eccd.6d41.e8f1	eth0.1034	–	dynamic	
192.168.2.2	eccd.6dd0.c136	eth0.2	–	dynamic	

Table 17: Parameters in the output of the **show arp** command

Parameter	Meaning
IP Address	IP address of the network device this entry maps to.
LL Address	Hardware address of the network device.
Interface	Interface over which the network device is accessed.
Port	Physical port that the network device is attached to.
Type	Whether the entry is a static or dynamic entry. Static entries are added using the arp command. Dynamic entries are learned from ARP request/reply message exchanges.

Related commands [arp](#)
[clear arp-cache](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

Version 5.4.9-0.1: Link layer addresses now shown as the hardware address (MAC Address output parameter has been renamed to LL Address).

show debugging ip packet

Overview Use this command to see what debugging is turned on for IP interfaces. IP interface debugging is set using the **debug ip packet interface** command.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax show debugging ip packet

Mode User Exec and Privileged Exec

Example To display the IP interface debugging status when the terminal monitor is off, use the commands:

```
awplus# terminal no monitor
awplus# show debugging ip packet
```

Output Figure 16-4: Example output from the **show debugging ip packet** command with **terminal monitor** off

```
awplus#terminal no monitor
awplus#show debugging ip packet
IP debugging status:
interface all tcp (stopped)
...
```

Example To display the IP interface debugging status when the terminal monitor is on, use the commands:

```
awplus# terminal monitor
awplus# show debugging ip packet
```

Output Figure 16-5: Example output from the **show debugging ip packet** command with **terminal monitor** on

```
awplus#terminal monitor
awplus#show debugging ip packet
IP debugging status:
interface all tcp (running)
...
```

Related commands [debug ip packet interface](#)
[terminal monitor](#)

show ip flooding-nexthops

Overview Use this command to display the static and dynamic ARP entries in the ARP cache that flood packets to multiple ports.

Syntax `show ip flooding-nexthops`

Mode User Exec and Privileged Exec

Example To display all of the flooding nexthop entries in the ARP cache, use the command:

```
awplus# show ip flooding-nexthops
```

Output Figure 16-6: Example output from **show ip flooding-nexthops**

awplus#show ip flooding-nexthops				
IP Address	MAC Address	Interface	Flooding Mode	Type
11.11.11.10	0300.0000.0011	eth0	port-group	static

Related commands [show arp](#)

Command changes Version 5.4.8-2.1: command added

show ip forwarding

Overview Use this command to display the IP forwarding status.

Syntax `show ip forwarding`

Mode User Exec and Privileged Exec

Example `awplus# show ip forwarding`

Output Figure 16-7: Example output from the **show ip forwarding** command

```
awplus#show ip forwarding
IP forwarding is on
```

Related commands [ip forwarding](#)

show ip interface

Overview Use this command to display information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip interface [<interface-list>] [brief]`

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. The specified interfaces must exist.

Mode User Exec and Privileged Exec

Examples To show the IP addresses assigned to ppp0, use the command:

```
awplus# show ip interface ppp0 brief
```

Output Figure 16-8: Example output from the **show ip interface brief** command

Interface	IP-Address	Status	Protocol
eth0	unassigned	admin up	running
eth0.3	192.168.3.1/24	admin up	running
eth0.2	192.168.2.1/24	admin up	running
lo	unassigned	admin up	running
br0	unassigned	admin up	down

show ip sockets

Overview Use this command to display information about the IP or TCP sockets that are present on the device. It includes TCP and UDP listen sockets, and displays the associated IP address and port.

The information displayed for established TCP sessions includes the remote IP address, port, and session state. Raw IP protocol listen socket information is also displayed for protocols such as VRRP and ICMP6, which are configured to receive IP packets with the associated protocol number.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip sockets`

Mode Privileged Exec

Usage notes Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Note that this command does not display sockets that are used internally for exchanging data between the various processes that exist on the device and are involved in its operation and management. It only displays sockets that are present for the purposes of communicating with other external devices.

Example To display IP sockets currently present on the device, use the command:

```
awplus# show ip sockets
```

Output Figure 16-9: Example output from **show ip sockets**

Socket information			
Not showing 40 local connections			
Not showing 7 local listening ports			
Typ	Local Address	Remote Address	State
tcp	0.0.0.0:111	0.0.0.0:*	LISTEN
tcp	0.0.0.0:80	0.0.0.0:*	LISTEN
tcp	0.0.0.0:23	0.0.0.0:*	LISTEN
tcp	0.0.0.0:443	0.0.0.0:*	LISTEN
tcp	0.0.0.0:4743	0.0.0.0:*	LISTEN
tcp	0.0.0.0:873	0.0.0.0:*	LISTEN
tcp	:::23	:::*	LISTEN
udp	0.0.0.0:111	0.0.0.0:*	
udp	226.94.1.1:5405	0.0.0.0:*	
udp	0.0.0.0:161	0.0.0.0:*	
udp	:::161	:::*	
raw	0.0.0.0:112	0.0.0.0:*	112
raw	:::58	:::*	58
raw	:::112	:::*	112

Table 16-1: Parameters in the output from **show ip sockets**

Parameter	Description
Not showing <number> local connections	This field refers to established sessions between processes internal to the device, that are used in its operation and management. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.
Not showing <number> local listening ports	This field refers to listening sockets belonging to processes internal to the device, that are used in its operation and management. They are not available to receive data from other devices. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.
Type	This column displays the type of the socket. Possible values for this column are: tcp : IP Protocol 6 udp : IP Protocol 17 raw : Indicates that socket is for a non port-orientated protocol (i.e. a protocol other than TCP or UDP) where all packets of a specified IP protocol type are accepted. For raw socket entries the protocol type is indicated in subsequent columns.
Local Address	For TCP and UDP listening sockets this shows the destination IP address and destination TCP or UDP port number for which the socket will receive packets. The address and port are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 or :: for IPv6. For active TCP sessions the IP address will display which of the devices addresses the session was established with. For raw sockets this displays the IP address and IP protocol for which the socket will accept IP packets. The address and protocol are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 and :: for IPv6. IP Protocol assignments are described at: www.iana.org/assignments/protocol-numbers

Table 16-1: Parameters in the output from **show ip sockets** (cont.)

Parameter	Description
Remote Address	For TCP and UDP listening sockets this shows the source IP address (either IPv4 or IPv6) and source TCP or UDP port number for which the socket will accept packets. The address and port are separated by ':'. If the socket will accept packets addressed from any IP address, the IP address will be 0.0.0.0 for IPv4. This is the usual case for a listening socket. Normally for a listen socket any source port will be accepted. This is indicated by '. For active TCP sessions the IP address will display the remote address and port the session was established with. For raw sockets the entry in this column will be 0.0.0.0: for IPv4.
State	This column shows the state of the socket. For TCP sockets this shows the state of the TCP state machine. For UDP sockets this column is blank. For raw sockets it contains the IP protocol number. The possible TCP states are: LISTEN SYN-SENT SYN-RECEIVED ESTABLISHED FIN-WAIT-1 FIN-WAIT-2 CLOSE-WAIT CLOSING LAST-ACK TIME-WAIT CLOSED RFC793 contains the TCP state machine diagram with Section 3.2 describing each of the states.

show ip traffic

Overview Use this command to display statistics regarding IP traffic sent and received by all interfaces on the device, showing totals for IP and IPv6 and then broken down into sub-categories such as TCP, UDP, ICMP and their IPv6 equivalents when appropriate.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax show ip traffic

Mode Privileged Exec

Example To display IP traffic statistics, use the command:

```
awplus# show ip traffic
```

Output Figure 16-10: Example output from the **show ip traffic** command

```
awplus#show ip traffic
IP:
    168475 packets received
    168475 delivered
    208099 sent
    35 dropped due to missing route
    22646409 bytes received
    126783216 bytes sent
    InCsumErrors 0
    InNoECTPkts 168475
    InECT1Pkts 0
    InECT0Pkts 0
    InCEPkts 0
    In107 Destination Unreachable
    Out11 Destination Unreachable
IPv6:
    14 packets received
    14 received packets delivered
    18 packets transmitted
...
ICMP6:
    4 messages sent
...
UDP6:
    Udp6RcvbufErrors 0
...
UDPLite6:
    UdpLite6RcvbufErrors 0
...
```

```
TCP:
    8 remote connections established
...
UDP:
    79797 datagrams received
...
UDPLite:
    InCsumErrors 0
...
```

tcpdump

Overview Use this command to start a tcpdump, which gives the same output as the Unix-like **tcpdump** command to display TCP/IP traffic. Press <ctrl> + c to stop a running tcpdump.

Syntax tcpdump <line>

Parameter	Description
<line>	Specify the dump options. For more information on the options for this placeholder see http://www.tcpdump.org/tcpdump_man.html

Mode Privileged Exec

Example To start a tcpdump running to capture IP packets, enter the command:

```
awplus# tcpdump ip
```

Output Figure 16-11: Example output from the **tcpdump** command

```
03:40:33.221337 IP 192.168.1.1 > 224.0.0.13: PIMv2, Hello,
length: 34
1 packets captured
2 packets received by filter
0 packets dropped by kernel
```

Related commands [debug ip packet interface](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

traceroute

Overview Use this command to trace the route to the specified IPv4 host.

Syntax `traceroute {<ip-addr>|<hostname>}`

Parameter	Description
<ip-addr>	The destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<hostname>	The destination hostname.

Mode User Exec and Privileged Exec

Example `awplus# traceroute 10.10.0.5`

Command changes Version 5.4.6-2.1: VRF-lite support added.

undebug ip packet interface

Overview This command applies the functionality of the no [debug ip packet interface](#) command.

17

Domain Name Service (DNS) Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Domain Name Service (DNS) features, including the following:

- DNS client
- DNS forwarding (DNS relay)
- Domain lists
- DDNS (Dynamic Domain Name System)

For more information about DNS and DDNS for AR-Series Firewalls, see the [Domain Name System \(DNS\) for AlliedWare Plus AR-Series Firewalls Feature Overview and Configuration Guide](#).

- Command List**
- ["accept-invalid-sslcert"](#) on page 512
 - ["clear ip dns forwarding cache"](#) on page 513
 - ["custom-failure"](#) on page 514
 - ["custom-success"](#) on page 515
 - ["ddns enable"](#) on page 516
 - ["ddns-update-method"](#) on page 517
 - ["ddns-update now"](#) on page 519
 - ["debug ddns"](#) on page 520
 - ["debug ip dns forwarding"](#) on page 521
 - ["description \(domain-list\)"](#) on page 522
 - ["domain"](#) on page 523
 - ["expect-html-response"](#) on page 524
 - ["follow-redirects"](#) on page 525
 - ["get-before-submit"](#) on page 526

- [“get-params”](#) on page 527
- [“host-name \(ddns-update-method\)”](#) on page 528
- [“ip ddns-update-method”](#) on page 529
- [“ip dns forwarding”](#) on page 530
- [“ip dns forwarding cache”](#) on page 531
- [“ip dns forwarding dead-time”](#) on page 532
- [“ip dns forwarding domain-list”](#) on page 533
- [“ip dns forwarding retry”](#) on page 534
- [“ip dns forwarding source-interface”](#) on page 535
- [“ip dns forwarding timeout”](#) on page 536
- [“ip domain-list”](#) on page 537
- [“ip domain-lookup”](#) on page 538
- [“ip domain-name”](#) on page 540
- [“ip name-server”](#) on page 541
- [“ip name-server preferred-order”](#) on page 543
- [“ipv6 ddns-update-method”](#) on page 544
- [“obey-form”](#) on page 545
- [“password \(ddns-update-method\)”](#) on page 546
- [“ppp ipcp dns”](#) on page 547
- [“ppp ipcp dns suffix-list”](#) on page 549
- [“retry-interval”](#) on page 551
- [“show ddns-update-method status”](#) on page 552
- [“show debugging ip dns forwarding”](#) on page 553
- [“show hosts”](#) on page 554
- [“show ip dns forwarding”](#) on page 555
- [“show ip dns forwarding cache”](#) on page 556
- [“show ip dns forwarding server”](#) on page 557
- [“show ip domain-list”](#) on page 558
- [“show ip domain-name”](#) on page 559
- [“show ip name-server”](#) on page 560
- [“suppress-ipv4-updates”](#) on page 561
- [“undebg ddns”](#) on page 562
- [“update-interval \(ddns-update-method\)”](#) on page 563
- [“update-url \(ddns-update-method\)”](#) on page 564
- [“use-ipv4-for-ipv6-updates”](#) on page 567

- [“username \(ddns-update-method\)”](#) on page 568

accept-invalid-sslcert

Overview Use this command to tell the dynamic DNS client to connect to an HTTPS server even if the server is producing an invalid SSL certificate (because it is self-signed, for a different host, expired, etc.).

Use the **no** variant of this command to return to the default.

Syntax `accept-invalid-sslcert`
`no accept-invalid-sslcert`

Default Not set

Mode Dynamic DNS Update Method Configuration

Example If the HTTPS server you are using for the dynamic DNS configuration "test" does not have a valid SSL certificate, then use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method test
awplus(config-ddns-update-method)# accept-invalid-sslcert
```

Command changes Version 5.5.0-0.1: command added

clear ip dns forwarding cache

Overview Use this command to clear the DNS Relay name resolver cache.

Syntax `clear ip dns forwarding cache`

Mode Privileged Exec

Examples To clear all cached data, use the command:

```
awplus# clear ip dns forwarding cache
```

Related commands [ip dns forwarding cache](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

custom-failure

Overview Use this command to specify the update server's failure message for Dynamic DNS. You only need to do this if the failure message is different to the ones in DDNS's built-in list.

Use the **no** variant of this command to remove the customized failure message.

Syntax `custom-failure <failure-word>`
`no custom-failure`

Parameter	Description
<code><failure-word></code>	A word that the update server sends to indicate a failed update.

Default No customized failure message

Mode Dynamic DNS Update Method Configuration

Example If the update server sends a message of 'AllBad' to indicate a failed update, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method test
awplus(config-ddns-update-method)# custom-failure AllBad
```

Related commands [custom-success](#)
[ddns-update-method](#)
[show ddns-update-method status](#)

Command changes Version 5.5.1-1.1: command added

custom-success

Overview Use this command to specify the update server's success message for Dynamic DNS. You only need to do this if the success message is different to the ones in DDNS's built-in list.

Use the **no** variant of this command to remove the customized success message.

Syntax `custom-success <success-word>`
`no custom-success`

Parameter	Description
<code><success-word></code>	A word that the update server sends to indicate a successful update.

Default No customized success message

Mode Dynamic DNS Update Method Configuration

Example If the update server sends a message of 'AllGood' to indicate a successful update, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method test
awplus(config-ddns-update-method)# custom-success AllGood
```

Related commands [custom-failure](#)
[ddns-update-method](#)
[show ddns-update-method status](#)

Command changes Version 5.5.1-1.1: command added

ddns enable

Overview Use this command to globally enable or disable DDNS updates. DDNS updates are disabled by default. DDNS configuration will remain when the updates are disabled and DDNS will still be configurable when updates are disabled.

Use the **no** variant of this command to disable DDNS updates.

Syntax `ddns enable`
`no ddns enable`

Default Disabled

Mode Global Configuration

Example To globally enable DDNS updates, use the commands:

```
awplus# configure terminal
awplus(config)# ddns enable
```

To globally disable DDNS updates, use the commands:

```
awplus# configure terminal
awplus(config)# no ddns enable
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

ddns-update-method

Overview Use this command to create a new DDNS update method and enter DDNS Update Method Configuration mode.

Use the **no** variant of this command to remove a DDNS update method.

Syntax `ddns-update-method <method-name>`
`no ddns-update-method <method-name>`

Parameter	Description
<code><method-name></code>	The name of the DDNS method.

Default None

Mode Global Configuration

Example To create a method named "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)#
```

Related commands

- [custom-failure](#)
- [custom-success](#)
- [ddns enable](#)
- [ddns-update now](#)
- [debug ddns](#)
- [expect-html-response](#)
- [host-name \(ddns-update-method\)](#)
- [ip ddns-update-method](#)
- [ipv6 ddns-update-method](#)
- [password \(ddns-update-method\)](#)
- [retry-interval](#)
- [show ddns-update-method status](#)
- [suppress-ipv4-updates](#)
- [update-interval \(ddns-update-method\)](#)
- [update-url \(ddns-update-method\)](#)
- [use-ipv4-for-ipv6-updates](#)
- [username \(ddns-update-method\)](#)

Command changes Version 5.4.7-0.1: command added

ddns-update now

Overview Use this command to manually update DDNS methods.

Syntax `ddns-update now`
`ddns-update method <method-name> now`

Parameter	Description
<method-name>	The DDNS update method name to use for the manual update.

Default None

Mode Privileged Exec

Usage notes When no method name is entered, all DDNS update methods are updated. If a method name is specified, then only that method will update.

Example To manually update all DDNS update methods, use the command:

```
awplus# ddns-update now
```

To manually update the method "dyndns", use the command:

```
awplus# ddns-update method dyndns now
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

debug ddns

- Overview** Use this command to enable debugging for the DDNS process.
Use the **no** variant of this command to disable debugging for the DDNS process.
- Syntax** `debug ddns`
`no debug ddns`
- Default** Disabled
- Mode** Privileged Exec
- Example** To enable debugging for the DDNS process, use the command:
`awplus# debug ddns`
To disable debugging for the DDNS process, use the command:
`awplus# no debug ddns`
- Related commands** [ddns-update-method](#)
[undebug ddns](#)
- Command changes** Version 5.4.7-0.1: command added

debug ip dns forwarding

Overview Use this command to enable DNS Relay debugging.
Use the **no** variant of this command to disable DNS Relay debugging.

Syntax `debug ip dns forwarding`
`no debug ip dns forwarding`

Default DNS Relay debugging is disabled by default.

Mode Privileged Exec

Examples To enable DNS forwarding debugging, use the commands:

```
awplus# debug ip dns forwarding
```

To disable DNS forwarding debugging, use the commands:

```
awplus# no debug ip dns forwarding
```

Related commands [ip dns forwarding](#)
[show debugging ip dns forwarding](#)

description (domain-list)

Overview Use this command to give a description to a domain-list.
Use the **no** variant of this command to delete the description.

Syntax `description <text>`
`no description`

Parameter	Description
<code><text></code>	Description string, 128 characters maximum. The string may contain spaces.

Mode Domain List

Usage notes When creating a domain-list, it is helpful to write a short description of what the list is to be used for.

Examples To add a description to a domain list, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list mydomains
awplus(config-domain-list)# description This is a useful
description of my domain list
```

To delete the description, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list mydomains
awplus(config-domain-list)# no description
```

Related commands [ip dns forwarding domain-list](#)

domain

Overview Use this command to add a domain to a domain list.
Use the **no** variant of this command to delete the domain.

Syntax `domain <domain-string>`
`no domain <domain-string>`

Parameter	Description
<code><domain-string></code>	• A domain name must only contain a-z, A-Z, 0-9, '-' (en-dash) and '.' (period) characters. • Each sub-section of the domain must not start or end with the '-' character. • Each sub-section must have no more than 64 characters including the '.'. • The last section must not have a '.' at the end. • The whole domain must be less than 254 characters long.

Mode Domain List

Usage notes Domain lists are objects that contain unsorted lists of domain names. After a domain list has been created, you can use this command to add domains to the domain list. There is no limit on the number of domains that can be added to a domain list.

Examples To add the domain "acme-solutions.com" to a domain list, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list acme-corporation
awplus(config-domain-list)# domain acme-solutions.com
```

To delete the domain, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list acme-corporation
awplus(config-domain-list)# no domain acme-solutions.com
```

Related commands [ip dns forwarding domain-list](#)

expect-html-response

Overview Use this command to allow Dynamic DNS to accept HTML formatted responses from the update server (and reject non-HTML responses). You need this if the update server sends HTML responses instead of plain text responses.

Use the **no** variant of this command to stop Dynamic DNS from accepting HTML responses.

Syntax `expect-html-response`
`no expect-html-response`

Default Disabled (HTML responses are rejected)

Mode Dynamic DNS Update Method Configuration

Example To configure DDNS to only accept an HTML response, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method test
awplus(config-ddns-update-method)# expect-html-response
```

Related commands [ddns-update-method](#)
[show ddns-update-method status](#)

Command changes Version 5.5.1-1.1: command added

follow-redirects

Overview Use this command to accept redirects during the initial GET request and during the update. See the command **get-before-submit**. The behavior without this command is to treat redirects as a failure.

Use the **no** variant of this command to disable following redirects.

Syntax follow-redirects
no follow-redirects

Default disabled

Mode Dynamic DNS Update Method Configuration

Example To configure DDNS to accept redirects, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# follow-redirects
```

Related commands [ddns-update-method](#)
[get-before-submit](#)
[obey-form](#)

Command changes Version 5.5.1-0.1: command added

get-before-submit

Overview Use this command to make DDNS perform a GET request for the page without any parameters before making the DDNS update submission.

Use the **no** variant of this command to disable this process.

Syntax `get-before-submit`
`no get-before-submit`

Default Disabled

Mode Dynamic DNS Update Method Configuration

Usage notes This command may be required if the service you are using either:

- follows a series of redirects before accepting the update submission (see the command **follow-redirects**).
- or
- if the update submission is normally submitted by the browser and contains either a CSRF token or Session ID (see the command **get-params**).

NOTE: Cookies from this GET request are used during the update submission.

Example To configure DDNS to perform a GET request for the page without any parameters before making the DDNS update submission, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# get-before-submit
```

Related commands [ddns-update-method](#)
[follow-redirects](#)
[get-params](#)
[obey-form](#)

Command changes Version 5.5.1-0.1: command added

get-params

Overview Use this command to support update services that use CSRF and other session tracking. This command picks up the required input fields and adds them to the request when it is sent.

Use the **no** variant of this command to remove parameters.

Syntax `get-params <parameter-name>`
`no get-params`

Parameter	Description
<code><parameter-name></code>	A comma separated list of input fields to include the values in the update.

Default No parameters are set

Mode Dynamic DNS Update Method Configuration

Usage notes During the **get-before-submit** stage, the HTML of the page is interpreted, and any input fields that match any of the names in the list are included as extra parameters when the update is submitted.

Example To configure the support update services that use CSRF, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# get-before-submit
awplus(config-ddns-update-method)# get-params session,csrf
```

Related commands [ddns-update-method](#)
[get-before-submit](#)

Command changes Version 5.5.1-0.1: command added

host-name (ddns-update-method)

Overview Use this command to add a host name for the current DDNS update method.

NOTE: A DDNS update method can only have one host name.

Use the **no** variant of this command to remove the host name from the current DDNS update method.

Syntax `host-name <host-name>`
`no host-name`

Parameter	Description
<code><host-name></code>	The name of the host to be configured in conjunction with the user name and password.

Default None

Mode Dynamic DNS Update Method Configuration

Example To add the host name "test.dyndns.org" for the DDNS update method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# host-name test.dyndns.org
```

To remove the host name "test.dyndns.org" from the DDNS update method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# no host-name
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

ip ddns-update-method

Overview Use this command to enable an IPv4 interface to update DDNS with the specified DDNS update method.

Use the **no** variant of this command to disable an IPv4 interface to update DDNS with the specified DDNS update method.

Syntax `ip ddns-update-method <method-name>`
`no ip ddns-update-method <method-name>`

Parameter	Description
<code><method-name></code>	A name given to a DDNS update method.

Default None

Mode Interface Configuration

Usage notes A DDNS update method cannot be attached to multiple interfaces, however multiple DDNS update methods can be assigned to the same interface.

Example To enable IPv4 DDNS updates for a DDNS update method named “dyndns” using interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip ddns-update-method dyndns
```

To disable IPv4 DDNS updates for a DDNS update method named “dyndns” using interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip ddns-update-method dyndns
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

ip dns forwarding

Overview Use this command to enable DNS Relay, the forwarding of incoming DNS queries for IP hostname-to-address translation.

Use the **no** variant of this command to disable the forwarding of incoming DNS queries for IP hostname-to-address translation.

Syntax `ip dns forwarding`
`no ip dns forwarding`

Default The forwarding of incoming DNS query packets is disabled by default.

Mode Global Configuration

Usage notes DNS Relay is independent of the configuration of [ip domain-lookup](#) (which is enabled by default). If [ip domain-lookup](#) is disabled, but DNS Relay is enabled, the router will continue to forward DNS queries by hosts in the network to its configured name-servers.

See the [ip dns forwarding dead-time](#) command used with this command.

Examples To enable the forwarding of incoming DNS query packets, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding
```

To disable the forwarding of incoming DNS query packets, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding
```

Related commands

- [clear ip dns forwarding cache](#)
- [debug ip dns forwarding](#)
- [ip dns forwarding cache](#)
- [ip dns forwarding dead-time](#)
- [ip dns forwarding retry](#)
- [ip dns forwarding source-interface](#)
- [ip dns forwarding timeout](#)
- [ip domain-lookup](#)
- [ip name-server](#)
- [show ip dns forwarding](#)
- [show ip dns forwarding cache](#)
- [show ip dns forwarding server](#)

ip dns forwarding cache

Overview Use this command to set the DNS Relay name resolver cache size and cache entry lifetime period. The DNS Relay name resolver cache stores the mappings between domain names and IP addresses.

Use the **no** variant of this command to set the default DNS Relay name resolver cache size and cache entry lifetime period.

Note that the lifetime period of the cache entry can be overwritten by the time-out period of the DNS reply from the DNS server if the time-out period of the DNS reply from the DNS server is smaller than the configured time-out period. The time-out period of the cache entry will only be used when the time-out period of the DNS reply from the DNS server is bigger than the time-out period configured on the device.

Syntax `ip dns forwarding cache [size <0-10000>] [timeout <60-3600>]`
`no ip dns forwarding cache [size|timeout]`

Parameter	Description
<0-10000>	Number of entries in the DNS Relay name resolver cache.
<60-3600>	Timeout value in seconds.

Default The default cache size is 0 (no entries) and the default lifetime is 1800 seconds.

Mode Global Configuration

Examples To set the cache size to 10 entries and the lifetime to 500 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding cache size 10 time 500
```

To set the cache size to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding cache size
```

Related commands

- [clear ip dns forwarding cache](#)
- [debug ip dns forwarding](#)
- [ip dns forwarding](#)
- [show ip dns forwarding](#)
- [show ip dns forwarding cache](#)

Command changes Version 5.4.8-1.1: maximum cache limit increased to 10000

ip dns forwarding dead-time

Overview Use this command to set the time period in seconds when the device stops sending any DNS requests to an unresponsive server and all retries set using [ip dns forwarding retry](#) are used. This time period is the DNS forwarding dead-time. The device stops sending DNS requests at the DNS forwarding dead-time configured and when all of the retries are used.

Use the **no** variant of this command to restore the default DNS forwarding dead-time value of 3600 seconds.

Syntax `ip dns forwarding dead-time <60-43200>`
`no ip dns forwarding retry`

Default The default time to stop sending DNS requests to an unresponsive server is 3600 seconds.

Mode Global Configuration

Usage notes See the [ip dns forwarding retry](#) command used with this command.

Examples To set the DNS forwarding retry count to 50 and to set the DNS forwarding dead-time to 1800 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dead-time 1800
awplus(config)# ip dns forwarding retry 50
```

To reset the DNS retry count to the default of 2 and the DNS forwarding dead-time to the default of 3600, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dead-time
awplus(config)# no ip dns forwarding retry
```

Related commands [debug ip dns forwarding](#)
[ip dns forwarding](#)
[ip dns forwarding retry](#)
[show ip dns forwarding](#)
[show ip dns forwarding server](#)

ip dns forwarding domain-list

Overview Use this command to create a domain-list that can be used as a suffix-list for DNS lookups. This command puts the device into a new mode where subsequent commands can be entered. The new mode is "Domain List Configuration" mode.

Use the **no** variant of this command to delete the domain-list.

Syntax `ip dns forwarding domain-list <domain-list-name>`
`no ip dns forwarding domain-list <domain-list-name>`

Parameter	Description
<code><domain-list-name></code>	Name of the list.

Mode Global Configuration

Usage notes The domain list can be used by features that need to match against domains. A domain list by itself does nothing; it must be attached to another feature to have functionality (like a prefix-list). For example, the domain list can be used as a suffix list on an DNS name-server. The DNS server can be either statically configured, or learned over a PPP connection.

Note that this command is separate from the **ip domain-list** command, which is used by DNS client to append a domain on to the end of a partial hostname to form a fully-qualified domain.

Examples To create a domain list to include domains that are internal to the company such as "engineering.acme" or "intranet.acme", use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
awplus(config-domain-list)# description internal network domain
awplus(config-domain-list)# domain engineering.acme
awplus(config-domain-list)# domain intranet.acme
```

To delete the domain list, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding domain-list
corporatedomains
```

Related commands [description \(domain-list\)](#)
[domain](#)
[ip name-server](#)
[ppp ipcp dns suffix-list](#)

ip dns forwarding retry

Overview Use this command to set the number of times DNS Relay will retry to forward DNS queries. The device stops sending DNS requests to an unresponsive server at the time set using the [ip dns forwarding dead-time](#) command and when all of the retries are used.

Use the **no** variant of this command to set the number of retries to the default of 2.

Syntax `ip dns forwarding retry <0-100>`
`no ip dns forwarding retry`

Default The default number of retries is 2 DNS requests to an unresponsive server.

Mode Global Configuration

Usage notes See the [ip dns forwarding dead-time](#) command used with this command.

Examples To set the DNS forwarding retry count to 50 and to set the DNS forwarding dead-time to 1800 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding retry 50
awplus(config)# ip dns forwarding dead-time 1800
```

To reset the DNS retry count to the default of 2 and the DNS forwarding dead-time to the default of 3600 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding retry
awplus(config)# no ip dns forwarding dead-time
```

Related commands [debug ip dns forwarding](#)
[ip dns forwarding](#)
[ip dns forwarding dead-time](#)
[show ip dns forwarding](#)

ip dns forwarding source-interface

Overview Use this command to set the interface to use for forwarding and receiving DNS queries.

Use the **no** variant of this command to unset the interface used for forwarding and receiving DNS queries.

Syntax `ip dns forwarding source-interface <interface-name>`
`no ip dns forwarding source-interface`

Parameter	Description
<code><interface-name></code>	An alphanumeric string that is the interface name.

Default The default is that no interface is set and the device selects the appropriate source IP address automatically.

Mode Global Configuration

Examples To set eth1.2 as the source interface for relayed DNS queries, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding source-interface eth1.2
```

To clear the source interface for relayed DNS queries, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding source-interface
```

Related commands [debug ip dns forwarding](#)
[ip dns forwarding](#)
[show ip dns forwarding](#)

ip dns forwarding timeout

Overview Use this command to set the time period for the DNS Relay to wait for a DNS response.

Use the **no** variant of this command to set the time period to wait for a DNS response to the default of 3 seconds.

Syntax `ip dns forwarding timeout <0-3600>`
`no ip dns forwarding timeout`

Default The default timeout value is 3 seconds.

Mode Global Configuration

Examples To set the timeout value to 12 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding timeout 12
```

To set the timeout value to the default of 3 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding timeout
```

Related commands [debug ip dns forwarding](#)
[ip dns forwarding](#)
[show ip dns forwarding](#)

ip domain-list

Overview This command adds a domain to the DNS list. Domains are appended to incomplete host names in DNS requests. Each domain in this list is tried in turn in DNS lookups. This list is ordered so that the first entry you create is checked first.

The **no** variant of this command deletes a domain from the list.

Syntax `ip domain-list <domain-name>`
`no ip domain-list <domain-name>`

Parameter	Description
<code><domain-name></code>	Domain string, for example "company.com".

Mode Global Configuration

Usage notes If there are no domains in the DNS list, then your device uses the domain specified with the [ip domain-name](#) command. If any domain exists in the DNS list, then the device does not use the domain set using the **ip domain-name** command.

Example To add the domain `example.net` to the DNS list, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-list example.net
```

Related commands [ip domain-lookup](#)
[ip domain-name](#)
[show ip domain-list](#)

ip domain-lookup

Overview This command enables the DNS client on your device. This allows you to use domain names instead of IP addresses in commands. The DNS client resolves the domain name into an IP address by sending a DNS inquiry to a DNS server, specified with the [ip name-server](#) command.

You can use the **via-relay** parameter to configure the DNS client to use the DNS relay for resolving domain lookups originating from the device. This setup is often preferred because the DNS relay offers additional features not available in the DNS client, such as caching, configurable timeout settings, and more.

The **no** variant of this command disables the DNS client. The client will not attempt to resolve domain names. You must use IP addresses to specify hosts in commands.

Syntax `ip domain-lookup [via-relay]`
`no ip domain-lookup`

Parameter	Description
via-relay	Perform resolution via DNS relay

Mode Global Configuration

Usage notes The client is enabled by default. However, it does not attempt DNS inquiries unless there is a DNS server configured.

Examples To enable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup
```

To configure the DNS client to perform resolution via the DNS relay, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup via-relay
awplus(config)# ip dns forwarding
```

To disable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip domain-lookup
```

Related commands

- [ip domain-list](#)
- [ip domain-name](#)
- [ip name-server](#)
- [show hosts](#)
- [show ip name-server](#)
- [ip dns forwarding](#)

Command changes Version 5.4.8-1.1: via-relay parameter added

ip domain-name

Overview This command sets a default domain for the DNS. The DNS client appends this domain to incomplete host-names in DNS requests.

The **no** variant of this command removes the domain-name previously set by this command.

Syntax `ip domain-name <domain-name>`
`no ip domain-name <domain-name>`

Mode Global Configuration

Usage notes If there are no domains in the DNS list (created using the [ip domain-list](#) command) then your device uses the domain specified with this command. If any domain exists in the DNS list, then the device does not use the domain configured with this command.

When your device is using its DHCP client for an interface, it can receive Option 15 from the DHCP server. This option replaces the domain name set with this command.

Example To configure the domain name, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-name company.com
```

Related commands [ip domain-list](#)
[show ip domain-list](#)
[show ip domain-name](#)

ip name-server

Overview Use this command to add IPv4 or IPv6 DNS server addresses. The DNS client on your device sends DNS queries to IP addresses in this list when trying to resolve a host name. Host names cannot be resolved until you have added at least one server to this list. A maximum of three name servers can be added to this list.

The **no** variant of this command removes the specified DNS name-server address.

Syntax `ip name-server <ip-addr> [suffix-list <domain-list>]`
`no ip name-server <ip-addr> [suffix-list]`

Parameter	Description
<code><ip-addr></code>	The IP address of the DNS server that is being added to the name server list. The address is entered in the form A.B.C.D for an IPv4 address, or in the form X:X::X:X for an IPv6 address. The order that you enter the servers in, is the order in which they will be used.
<code>suffix-list</code>	Specify domain suffixes that should be directed to this name server
<code><domain-list></code>	The name of the DNS domain-list

Mode Global Configuration

Usage notes To allow the device to operate as a DNS proxy, your device must have learned about a DNS name-server to forward requests to. Name-servers can be learned through the following means:

- Manual configuration, using the **ip name-server** command
- Learned from DHCP server with Option 6
- Learned over a PPP tunnel if the neighbor advertises the DNS server

Use this command to statically configure a DNS name-server for the device to use.

The order that you enter the servers in, is the order in which they will be used.

For more information about PPP and DNS, see the [PPP Feature Overview and Configuration Guide](#).

Examples To allow a device to send DNS queries to a DNS server with the IPv4 address 10.10.10.5, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server 10.10.10.5
```

To enable your device to send DNS queries to a DNS server with the IPv6 address 2001:0db8:010d::1, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server 2001:0db8:010d::1
```

For DNS relay, to direct DNS lookups for domains with suffixes of "engineering.acme" or "intranet.acme" to an internal corporate name-server, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
awplus(config-domain-list)# description Our internal network
domains; do not send DNS requests to internet
awplus(config-domain-list)# domain engineering.acme
awplus(config-domain-list)# domain intranet.acme
awplus(config-domain-list)# exit
awplus(config)# ip name-server 172.16.0.1 suffix-list
corporatedomains
```

**Related
commands**

[ip dns forwarding](#)
[ip dns forwarding domain-list](#)
[ip domain-list](#)
[ip domain-lookup](#)
[ip domain-name](#)
[show ip dns forwarding cache](#)
[show ip name-server](#)

**Command
changes**

Version 5.4.6-2.1: VRF-lite support added to AR-series devices.

ip name-server preferred-order

Overview Use this command to choose between using statically-configured DNS servers or dynamically-learned DNS servers.

Use the **no** variant of this command to set the DNS servers back to the default setting of dynamic.

Syntax `ip name-server preferred-order {dynamic|static}`
`no ip name-server preferred-order`

Parameter	Description
dynamic	Use dynamically learned DNS servers first.
static	Use statically configured DNS servers first.

Default dynamic

Mode Global Configuration

Usage notes This command is used to choose which DNS server set to use first. Select either the **dynamic** or **static** parameter.

Examples To configure the preference to use static servers first, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server preferred-order static
```

To configure the preference to use dynamically-learned servers first, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server preferred-order dynamic
```

or

```
awplus# configure terminal
awplus(config)# no ip name-server preferred-order
```

Related commands [ip address dhcp](#)
[ip name-server](#)
[ipv6 address dhcp](#)
[ppp ipcp dns](#)
[show ip name-server](#)

Command changes Version 5.4.9-0.1: command added

ipv6 ddns-update-method

Overview Use this command to enable an IPv6 interface to update DDNS with the specified DDNS update method.

Use the **no** variant of this command to disable an IPv6 interface to update DDNS with the specified DDNS update method.

Syntax `ipv6 ddns-update-method <method-name>`
`no ipv6 ddns-update-method <method-name>`

Parameter	Description
<code><method-name></code>	A name given to a DDNS update method.

Default None

Mode Interface Configuration

Usage notes A DDNS update method cannot be attached to multiple interfaces, however multiple DDNS update methods can be assigned to the same interface.

Example To enable IPv6 DDNS updates for a DDNS update method named “dyndns” using interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ddns-update-method dyndns
```

To disable IPv6 DDNS updates for a DDNS update method named “dyndns” using interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 ddns-update-method dyndns
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

obey-form

Overview Use this command to read the action URL from the form and submit to that URL instead of the current page's URL. This is needed for forms that don't submit to the current page's URL.

Use the **no** variant of this command to disable form submission.

Syntax `obey-form`
`no obey-form`

Default Disabled

Mode Dynamic DNS Update Method Configuration

Usage notes This command applies after the **follow-redirects** and **get-before-submit** commands are applied.

Example To turn on obey-form, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# get-before-submit
awplus(config-ddns-update-method)# obey-form
```

Related commands [ddns-update-method](#)
[get-before-submit](#)
[follow-redirects](#)

Command changes Version 5.5.0.1: command added

password (ddns-update-method)

Overview Use this command to add a password to the current DDNS update method.

Use the **no** variant of this command to remove a password from the current DDNS update method.

Syntax password <password>
no password

Parameter	Description
<password>	The password to be configured in conjunction with the user name and host name.

Default None

Mode Dynamic DNS Update Method Configuration

Example To configure the password "test" for the method "dyndns", use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# password test
```

To remove the password "test" from the method "dyndns", use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# no password
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

ppp ipcp dns

Overview Use this command to configure the primary and secondary DNS (Domain Name System) IP addresses for IPCP (Internet Protocol Control Protocol) on a given PPP interface.

Use the **no** variant of this command to remove the primary and secondary DNS IP addresses for IPCP on a given PPP interface, and remove any optional parameters configured for DNS.

Syntax `ppp ipcp dns [<primary> [<secondary>]] [required|reject|request]`
`no ppp ipcp dns`

Parameter	Description
<primary>	Specify the primary DNS address for a given PPP interface to the peer.
<secondary>	Specify the secondary DNS address for a given PPP interface to the peer.
required	Request DNS addresses from the peer, and close the link if none is given.
reject	Reject negotiations with the peer (default).
request	Request DNS addresses from the peer.

Default By default no IPCP DNS server request is sent to the peer.

Mode Interface Configuration

Usage notes Use the optional parameters to configure PPP IPCP DNS options for accepting, rejecting or requesting DNS addresses from the peer. Use the optional primary and secondary or primary only DNS server address placeholders to specify DNS server addresses to the peer.

The no variant of this command also stops IPCP DNS request messages being sent to the peer.

Examples To configure the PPP interface `ppp0` to require a DNS IP address from the peer, and close the link if a DNS IP address is not given, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns required
```

To configure the PPP interface `ppp0` to require a DNS IP address from the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns request
```

To configure the PPP interface `ppp0` to reject a DNS IP address from the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns reject
```

To configure the PPP interface `ppp0` to supply primary and secondary DNS server addresses to the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns 10.1.1.2 10.1.1.3
```

To configure the PPP interface `ppp0` to supply a primary but not a secondary DNS server address to the peer, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns 10.1.1.2
```

**Related
commands**

[ip address negotiated](#)
[peer default ip address](#)
[peer neighbor-route](#)
[show running-config interface](#)

ppp ipcp dns suffix-list

Overview Use this command to configure a suffix-list to be associated with DNS name-servers learned over the PPP connection.

Use the **no** variant of this command to remove the suffix-list.

Syntax `ppp ipcp dns suffix-list <domain-list-name>`
`no ppp ipcp dns suffix-list`

Parameter	Description
<code><domain-list-name></code>	The name of the DNS domain-list

Mode Interface Configuration

Usage notes A PPP connection can be configured to learn DNS servers from the remote peer by using the command `ppp ipcp dns` command.

This command allows a user to associate a domain-list to be used to match against the suffixes of incoming DNS requests. For example, a customer branch office may have a router that is used to give remote-access to their head office, over which they learn the IP address of the head office's DNS server. A domain list can be created that contains a suffix used for services internal to that company, for example, "example.lc". This domain-list is associated as a suffix-list to the PPP connection. So when the PPP connection is completed with the head office, users at the branch office that browse to "intranet.example.lc" will have the DNS request forwarded to the DNS server learned over the PPP connection. Without having the suffix-list configured, the DNS request for "intranet.example.lc" would instead be sent to the primary DNS server, which is likely to be the branch office's ISP, and they will simply respond with a negative reply, because .example.lc is not a globally routable domain.

Examples At a branch office, to direct DNS lookups for domains with suffixes of "engineering.acme" or "intranet.acme" to an internal corporate name-server run at head-office that was learned over a PPP connection, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
host(config-domain-list)# description Our internal network
domains; do not send DNS requests to internet
host(config-domain-list)# domain engineering.acme
host(config-domain-list)# domain intranet.acme
awplus(config)# interface ppp0
awplus(config-if)# ppp ipcp dns required
awplus(config-if)# ppp ipcp dns suffix-list corporatedomains
```

Related commands [ip dns forwarding domain-list](#)
[ppp ipcp dns](#)

retry-interval

Overview Use this command to enable DDNS update retries. Retries are attempted after a DDNS update fails after the specified interval. If the DDNS update keeps failing, then no more than the specified maximum retries are attempted.

NOTE: *The retry interval is used for one DDNS update at one time, so if an update is not complete within the specified interval, an update will not begin until it has completed.*

Use the **no** variant of this command to disable DDNS update retries.

Syntax `retry-interval <1-3888000> maximum-retries <1-100>`
`no retry-interval`

Parameter	Description
<1-3888000>	The retry interval in seconds (from 1 second to 4.5 days), after which a failed DDNS update will be retried.
<1-100>	The maximum number of times a retry is allowed.

Default Disabled

Mode Dynamic DNS Update Method Configuration

Usage notes If an update is triggered by another source, such as an IP address change or a manual update, then the retry counter will start again from the beginning.

Example To enable DDNS update retry attempts every hour up to 5 times for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# retry-interval 3600
maximum-retries 5
```

To disable DDNS update retry attempts for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# no retry-interval
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

show ddns-update-method status

Overview Use this command to show the status of the configured DDNS update methods.

Syntax `show ddns-update-method status`

Mode User Exec and Privileged Exec

Example To display the status of DDNS update methods currently configured on your device, use the command:

```
awplus# show ddns-update-method status
```

Output Figure 17-1: Example output from **show ddns-update-method status**

```
awplus#show ddns-update-method status

Dynamic DNS updates are enabled

-----
Update Method Name      test
Hostname                 test.dnsalias.org
IPv4 Interface          eth1
IPv4 Address             192.168.10.100
IPv4 Status              Update succeeded
IPv4 Update Result       good 192.168.10.100
IPv6 Interface          eth1
IPv6 Address             333::f195
IPv6 Status              Update succeeded
IPv6 Update Result       good 0333:0000:0000:0000:0000:0000:f195
Last update              Last update Mar 25, 2022 06:54:24
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

show debugging ip dns forwarding

Overview Use this command to see what debugging is turned on for DNS Relay. DNS Relay debugging is set using the **debug ip dns forwarding** command.

For information on filtering and saving command output, see the [“Getting_Started with AlliedWare Plus” Feature Overview and Configuration_Guide](#).

Syntax `show debugging ip dns forwarding`

Mode User Exec and Privileged Exec

Example To display the DNS Relay debugging status, use the command:

```
awplus# show debugging ip dns forwarding
```

Output Figure 17-2: Example output from the **show debugging ip dns forwarding** command:

```
awplus#show debugging ip dns forwarding

DNS Relay debugging status:
  debugging is on
```

Related commands [debug ip dns forwarding](#)

show hosts

Overview This command shows the default domain, domain list, and name servers configured on your device.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show hosts`

Mode User Exec and Privileged Exec

Example To display the default domain, use the command:

```
awplus# show hosts
```

Output Figure 17-3: Example output from the **show hosts** command when **no ip domain-lookup** is configured

```
awplus#show hosts

Default domain is not set
Name/address lookup is disabled
```

Figure 17-4: Example output from the **show hosts** command when **ip domain-lookup** is configured

```
awplus#show hosts

Default domain is mycompany.com
Domain list: company.com
Name/address lookup uses domain service
Name servers are 10.10.0.2 10.10.0.88
```

Figure 17-5: Example output from the **show hosts** command when **ip domain-lookup via-relay** is configured

```
awplus#show hosts

Default domain is mycompany.com
Domain list: company.com
Name/address lookup uses domain relay service
Name servers are 10.10.0.2 10.10.0.88
```

Related commands

- [ip domain-list](#)
- [ip domain-lookup](#)
- [ip domain-name](#)
- [ip name-server](#)

show ip dns forwarding

Overview Use this command to display the DNS Relay status.

Syntax `show ip dns forwarding`

Mode User Exec and Privileged Exec

Examples To display the DNS Relay status, use the command:

```
awplus# show ip dns forwarding
```

Output Figure 17-6: Example output from the **show ip dns forwarding** command

```
awplus#show ip dns forwarding

Max-Retry      : 2
Timeout        : 3 second(s)
Dead-Time      : 3600 second(s)
Source-Interface: not specified
DNS Cache      : disabled
```

Related commands [ip dns forwarding](#)

show ip dns forwarding cache

Overview Use this command to display the DNS Relay name resolver cache.

Syntax `show ip dns forwarding cache`

Mode User Exec and Privileged Exec

Example To display the DNS Relay name resolver cache, use the command:

```
awplus# show ip dns forwarding cache
```

Output Figure 17-7: Example output from the **show ip dns forwarding cache** command

```
awplus#show ip dns forwarding cache
IPv4 addresses in cache:      3
IPv6 addresses in cache:      0
Cache size: 1000
Host                          Address                      Expires  Flags
www.example.com               172.16.1.1.                 180
mail.example.com               www.example.com              180  CNAME
www.example.com               172.16.1.1.                 180  REVERSE
mail.example.com               172.16.1.5.                 180
```

Related commands [ip dns forwarding cache](#)
[ip name-server](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.
Version 5.4.8-1.1: additional cache counters added to output.

show ip dns forwarding server

Overview Use this command to display the status of DNS forwarding name servers.

Syntax `show ip dns forwarding server`

Parameter	Description
forwarding server	Display information about the DNS forwarding name servers.

Mode User Exec and Privileged Exec

Examples To display the status of DNS Relay name servers, use the command:

```
awplus# show ip dns forwarding server
```

Output Figure 17-8: Example output from the **show ip dns forwarding server** command

awplus#show ip dns forwarding server			
Servers	Forwards	Fails	Dead-Time
172.16.1.1	12	0	active
172.16.1.2	6	3	3900

Related commands [ip dns forwarding](#)
[ip dns forwarding dead-time](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

show ip domain-list

Overview This command shows the domains configured in the domain list. The DNS client uses the domains in this list to append incomplete hostnames when sending a DNS inquiry to a DNS server.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip domain-list`

Mode User Exec and Privileged Exec

Example To display the list of domains in the domain list, use the command:

```
awplus# show ip domain-list
```

Output Figure 17-9: Example output from the **show ip domain-list** command

```
awplus#show ip domain-list
alliedtelesis.com
mycompany.com
```

Related commands [ip domain-list](#)
[ip domain-lookup](#)

show ip domain-name

Overview This command shows the default domain configured on your device. When there are no entries in the DNS list, the DNS client appends this domain to incomplete hostnames when sending a DNS inquiry to a DNS server.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip domain-name`

Mode User Exec and Privileged Exec

Example To display the default domain configured on your device, use the command:

```
awplus# show ip domain-name
```

Output Figure 17-10: Example output from the **show ip domain-name** command

```
awplus#show ip domain-name  
alliedtelesis.com
```

Related commands [ip domain-name](#)
[ip domain-lookup](#)

show ip name-server

Overview This command displays a list of IPv4 and IPv6 DNS server addresses that your device will send DNS requests to. This is a static list configured using the [ip name-server](#) command.

The command will also show any domain-list that has been associated as suffix-list with the DNS server, and the domains that will be preferentially directed to that DNS server.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip name-server`

Mode User Exec and Privileged Exec

Example To display the list of DNS servers that your device sends DNS requests to, use the command:

```
awplus# show ip name-server
```

Output Figure 17-11: Example output from the **show ip name-server** command

```
awplus#show ip name-server
Currently learned name-servers
10.36.200.165 dynamic (ppp0)
10.35.12.20 dynamic (ppp1), using suffix-list mysuffixlist:
    test.com
    intranet.interslice.com
10.37.84.97 static
130.37.84.97 static
```

Related commands [ip domain-lookup](#)
[ip name-server](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

suppress-ipv4-updates

Overview Use this command to suppress IPv4 updates from being sent.

Use the **no** variant of this command to stop suppressing IPv4 updates from being sent.

Syntax `suppress-ipv4-updates`
`no suppress-ipv4-updates`

Default Disabled

Mode Dynamic DNS Update Method Configuration

Usage notes This command is used in conjunction with the **use-ipv4-for-ipv6-updates** command. IPv4 DDNS updates are suppressed so that only IPv6 updates are sent.

NOTE: *The IPv4 DNS entry may be updated using the source IPv4 address used.*

Example To suppress IPv4 updates and send IPv6 updates instead for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method-dyndns
awplus(config-ddns-update-method)# use-ipv4-for-ipv6-updates
awplus(config-ddns-update-method)# suppress-ipv4-updates
```

Related commands [ddns-update-method](#)
[use-ipv4-for-ipv6-updates](#)

Command changes Version 5.4.7-0.1: command added

undebug ddns

Overview Use this command to disable debugging for the DDNS process.

Syntax undebug ddns

Default Disabled

Mode Privileged Exec

Example To disable debugging for the DDNS process, use the command:

```
awplus# undebug ddns
```

Related commands [ddns-update-method](#)
[debug ddns](#)

Command changes Version 5.4.7-0.1: command added

update-interval (ddns-update-method)

Overview Use this command to specify the time interval between periodic DDNS updates.
Use the **no** variant of this command to disable periodic DDNS updates.

Syntax `update-interval <1-64800>`
`no update-interval`

Parameter	Description
<code><1-64800></code>	Update interval time in minutes (from 1 minute to 45 days).

Default Disabled

Mode Dynamic DNS Update Method Configuration

Examples To enable periodic DDNS updates every day for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# update-interval 1440
```

To enable periodic DDNS updates every 28 days for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# update-interval 40320
```

To disable periodic DDNS updates for the method "dyndns", use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# no update-interval
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

update-url (ddns-update-method)

Overview Use this command to configure a URL for DDNS updates for the current DDNS update method.

Use the **no** variant of this command to remove an update URL from a DDNS update method.

Syntax `update-url <url-name>`
`no update-url <url-name>`

Parameter	Description
<code><url-name></code>	The update URL is provided by the DDNS provider and can be configured with the following placeholder tokens: • <code><USERNAME></code> • <code><PASSWORD></code> • <code><HOST-NAME></code> • <code><IPADDRESS></code> To specify the values for <code><USERNAME></code> , <code><PASSWORD></code> and <code><HOST-NAME></code> , use the commands username , password and hostname . The value for <code><IPADDRESS></code> is populated automatically from the interface IP settings.

Default None

Mode Dynamic DNS Update Method Configuration

Usage notes The update URL (provided by the DDNS provider) can include a user name, password, host name and/or IP address. These user values are optional because they may vary depending on the DDNS provider's update URLs. AlliedWare Plus requires you to enter the required parameters for the update URL using the following placeholder tokens:

- for the user name enter "`<USERNAME>`"
- for the password enter "`<PASSWORD>`"
- for the host name enter "`<HOST-NAME>`"
- for the IP address enter "`<IPADDRESS>`"

For example, for DynDNS the following update URL can be used:

```
http://username:password@members.dyndns.org/nic/update?  
SYSTEM=dyndns&hostname=<h>&myip=<a>
```

To configure this URL, use the following command including the placeholder tokens as written here:

```
awplus(config-ddns-update-method)# update-url  
http://<USERNAME>:<PASSWORD>@members.dyndns.org/nic/update?  
SYSTEM=dyndns&hostname=<HOST-NAME>&myip=<IPADDRESS>
```


DynDNS also has the following update URL that can be used instead:

```
http://<USERNAME>:<PASSWORD>@members.dyndns.org/v3/update?  
hostname=<HOST-NAME>&myip=<IPADDRESS>
```

NOTE: URLs that contain the character "?" activate help from the command line. To stop the help from activating enter the "?" in the command line, then press Ctrl+v.

For more information and examples, see the [Domain Name System \(DNS\) for AlliedWare Plus AR-Series Firewalls Feature Overview and Configuration Guide](#).

Examples To use members.dyndns.org/nic/update as the update URL for the provider DynDNS, with the method called "dyndns" that uses HTTP, use the following commands:

```
awplus# configure terminal  
awplus(config)# ddns-update-method dyndns  
awplus(config-ddns-update-method)# update-url  
http://<USERNAME>:<PASSWORD>@members.dyndns.org/nic/update?  
SYSTEM=dyndns&hostname=<HOST-NAME>&myip=<IPADDRESS>
```

To use members.dyndns.org/v3/update as the update URL for the provider DynDNS, with the method called "dyndns" that uses HTTP, use the following commands:

```
awplus# configure terminal  
awplus(config)# ddns-update-method dyndns  
awplus(config-ddns-update-method)# update-url  
http://<USERNAME>:<PASSWORD>@members.dyndns.org/v3/update?  
hostname=<HOST-NAME>&myip=<IPADDRESS>
```

To use members.dyndns.org/v3/update as the update URL for the provider DynDNS, with the method called "dyndns" that uses HTTPS/SSL, use the following commands:

```
awplus# configure terminal  
awplus(config)# ddns-update-method dyndns  
awplus(config-ddns-update-method)# update-url  
https://<USERNAME>:<PASSWORD>@members.dyndns.org/v3/update?  
hostname=<HOST-NAME>&myip=<IPADDRESS>
```

To use members.dyndns.org/v3/update as the update URL for the provider DynDNS, with the method called "dyndns" that uses HTTP on port 8245, use the following commands:

```
awplus# configure terminal  
awplus(config)# ddns-update-method dyndns  
awplus(config-ddns-update-method)# update-url  
http://<USERNAME>:<PASSWORD>@members.dyndns.org:8245/v3/  
update?hostname=<HOST-NAME>&myip=<IPADDRESS>
```

To remove the update URL from the method called “dyndns”, use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# no update-url
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

use-ipv4-for-ipv6-updates

Overview Use this command to send IPv6 updates using IPv4.
Use the **no** variant of this command to stop sending IPv6 updates using IPv4.

Syntax `use-ipv4-for-ipv6-updates`
`no use-ipv4-for-ipv6-updates`

Default Disabled

Mode Dynamic DNS Update Method Configuration

Usage notes If your DDNS provider supports IPv6 but does not support sending updates in IPv6 then this command is used so IPv6 updates can be sent using IPv4 instead. The **suppress-ipv4-updates** command is used in conjunction with this command to suppress IPv4 updates and send only IPv6 updates instead.

example To send IPv6 updates using IPv4 for the method "dyndns" and to suppress IPv4 updates, use the commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# use-ipv4-for-ipv6-updates
awplus(config-ddns-update-method)# suppress-ipv4-updates
```

Related commands [ddns-update-method](#)
[suppress-ipv4-updates](#)

Command changes Version 5.4.7-0.1: command added

username (ddns-update-method)

Overview Use this command to add a user name to the current DDNS update method.

Use the **no** variant of this command to remove a user name from the current DDNS update method.

Syntax `username <user-name>`
`no username`

Parameter	Description
<code><user-name></code>	The name of the user to be configured in conjunction with the password and host name.

Default None

Mode Dynamic DNS Update Method Configuration

Example To configure the username "atlnz" for the method "dyndns", use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# username atlnz
```

To remove the username "atlnz" from the method "dyndns", use the following commands:

```
awplus# configure terminal
awplus(config)# ddns-update-method dyndns
awplus(config-ddns-update-method)# no username
```

Related commands [ddns-update-method](#)

Command changes Version 5.4.7-0.1: command added

18

IPv6 Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure IPv6. For more information, see the [IPv6 Feature Overview and Configuration Guide](#).

- Command List**
- [“clear ipv6 neighbors”](#) on page 571
 - [“ipv6 address”](#) on page 572
 - [“ipv6 address autoconfig”](#) on page 574
 - [“ipv6 address suffix”](#) on page 576
 - [“ipv6 enable”](#) on page 577
 - [“ipv6 eui64-linklocal”](#) on page 579
 - [“ipv6 forwarding”](#) on page 580
 - [“ipv6 icmp error-interval”](#) on page 581
 - [“ipv6 multicast forward-slow-path-packet”](#) on page 582
 - [“ipv6 multihoming”](#) on page 583
 - [“ipv6 nd accept-ra-default-routes”](#) on page 584
 - [“ipv6 nd accept-ra-pinfo”](#) on page 585
 - [“ipv6 nd current-hoplimit”](#) on page 586
 - [“ipv6 nd dns search-list”](#) on page 588
 - [“ipv6 nd dns-server”](#) on page 589
 - [“ipv6 nd managed-config-flag”](#) on page 591
 - [“ipv6 nd minimum-ra-interval”](#) on page 592
 - [“ipv6 nd other-config-flag”](#) on page 594
 - [“ipv6 nd prefix”](#) on page 595

- ["ipv6 nd proxy interface"](#) on page 597
- ["ipv6 nd ra-interval"](#) on page 598
- ["ipv6 nd ra-lifetime"](#) on page 599
- ["ipv6 nd reachable-time"](#) on page 601
- ["ipv6 nd retransmission-time"](#) on page 603
- ["ipv6 nd route-information"](#) on page 605
- ["ipv6 nd router-preference"](#) on page 606
- ["ipv6 nd suppress-ra"](#) on page 607
- ["ipv6 opportunistic-nd"](#) on page 608
- ["ipv6 route"](#) on page 609
- ["ipv6 unreachable"](#) on page 611
- ["ping ipv6"](#) on page 612
- ["show ipv6 forwarding"](#) on page 614
- ["show ipv6 interface"](#) on page 615
- ["show ipv6 neighbors"](#) on page 616
- ["show ipv6 route"](#) on page 617
- ["show ipv6 route summary"](#) on page 619
- ["traceroute ipv6"](#) on page 620

clear ipv6 neighbors

Overview Use this command to clear all dynamic IPv6 neighbor entries.

Syntax `clear ipv6 neighbors`

Mode Privileged Exec

Example `awplus# clear ipv6 neighbors`

Related commands [show ipv6 neighbors](#)

ipv6 address

Overview Use this command to set the IPv6 address of an interface. The command also enables IPv6 on the interface, which creates an EUI-64 link-local address as well as enabling RA processing and SLAAC.

To stop the device from processing prefix information (routes and addresses from the received Router Advertisements) use the command **no ipv6 nd accept-ra-pinfo**.

To remove the EUI-64 link-local address, use the command **no ipv6 eui64-linklocal**.

Use the **no** variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

Syntax `ipv6 address <ipv6-addr/prefix-length>`
`no ipv6 address <ipv6-addr/prefix-length>`

Parameter	Description
<code><ipv6-addr/prefix-length></code>	Specifies the IPv6 address to be set. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them. See the [ipv6 enable](#) command for more information.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the [ipv6 enable](#) command then it will not be removed using a **no ipv6 address** command.

Examples To assign the IPv6 address 2001:0db8::a2/64 to eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```


To assign the IPv6 address to the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To assign the IPv6 address to the tunnel tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

**Related
commands**

[ipv6 address autoconfig](#)

[ipv6 address dhcp](#)

[ipv6 dhcp server](#)

[ipv6 enable](#)

[ipv6 eui64-linklocal](#)

[show running-config](#)

[show ipv6 interface](#)

[show ipv6 route](#)

ipv6 address autoconfig

Overview Use this command to enable IPv6 stateless address autoconfiguration (SLAAC) for an interface. This configures an IPv6 address on an interface derived from the MAC address on the interface.

Use the **no** variant of this command to disable IPv6 SLAAC on an interface. Note that if no global addresses are left after removing all IPv6 autoconfigured addresses then IPv6 is disabled.

Syntax `ipv6 address autoconfig`
`no ipv6 address autoconfig`

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes Use this command to enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface, and enable IPv6.

IPv6 hosts can configure themselves when connected to an IPv6 network using ICMPv6 (Internet Control Message Protocol version 6) router discovery messages. Configured routers respond with a Router Advertisement (RA) containing configuration parameters for IPv6 hosts.

The SLAAC process derives the interface identifier of the IPv6 address from the MAC address of the interface.

If SLAAC is not suitable then a network can use stateful configuration with DHCPv6 (Dynamic Host Configuration Protocol version 6) Relay, or hosts can be configured statically. See [ip dhcp-relay server-address](#) for the DHCPv6 Relay server command description and examples. See the [IP Feature Overview and Configuration Guide](#) for more information about DNS Relay.

Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them. See the [ipv6 enable](#) command for more information.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the [ipv6 enable](#) command then it will not be removed using a **no ipv6 address** command.

Examples To enable SLAAC on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 address autoconfig
```

To disable SLAAC on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 address autoconfig
```

**Related
commands**

[ipv6 address](#)
[ipv6 enable](#)
[show ipv6 interface](#)
[show running-config](#)

ipv6 address suffix

Overview Use this command to configure the suffix to use when generating an address from prefix information. Any addresses that were created with the EUI-64 suffix will be removed, and new addresses will be added after the next Router Advertisement.

Use the **no** variant of this command to set it back to the default of disabled or set to `::` for the same result as the **no** variant.

Syntax `ipv6 address suffix <ipv6-addr-suffix>`
`no ipv6 address suffix`

Parameter	Description
<code><ipv6-addr-suffix></code>	In the format of <code>::X:X:X:X</code> , for example <code>::a2d8:0fd8</code>

Default Disabled

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To configure the suffix to use when generating an address from prefix information on eth0, use the command:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 address suffix ::a2d8:0fd8
```

Related commands [ipv6 nd accept-ra-pinfo](#)
[show running-config interface](#)

Command changes Version 5.4.8-2.1: command added

ipv6 enable

Overview Use this command to enable automatic configuration of a link-local IPv6 address on an interface using Stateless Automatic Address Configuration (SLAAC). By default, the EUI-64 method is used to generate the link-local address.

Use the **no** variant of this command to disable IPv6 on an interface without a global address. Note, to stop EUI-64 from generating the automatic link-local address, use the command **no ipv6 eui64-linklocal**.

Syntax `ipv6 enable`
`no ipv6 enable`

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes The **ipv6 enable** command automatically configures an IPv6 link-local address on the interface and enables the interface for IPv6 processing.

A link-local address is an IP (Internet Protocol) address that is only used for communications in the local network, or for a point-to-point connection. Routing does not forward packets with link-local addresses. IPv6 requires that a link-local address is assigned to each interface that has the IPv6 protocol enabled, and when addresses are assigned to interfaces for routing IPv6 packets.

Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the **ipv6 enable** command then it will not be removed using a **no ipv6 address** command.

Default All interfaces default to IPv6-down with no address.

Examples To enable IPv6 with only a link-local IPv6 address on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 enable
```

To enable IPv6 with only a link-local IPv6 address on the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 enable
```

**Related
commands**

- [ipv6 address](#)
- [ipv6 address autoconfig](#)
- [ipv6 address dhcp](#)
- [ipv6 address \(DHCPv6 PD\)](#)
- [ipv6 dhcp client pd](#)
- [ipv6 nd prefix](#)
- [show ipv6 interface](#)
- [show ipv6 route](#)
- [show running-config](#)

ipv6 eui64-linklocal

Overview When IPv6 is enabled on an interface, an EUI link-local address is generated and installed on the interface. In other words, **ipv6 eui64-linklocal** is enabled by default on any IPv6 enabled interface.

Use the **no** variant of this command to disallow the automatic generation of the EUI-64 link-local address on an IPv6 enabled interface.

Syntax `ipv6 eui64-linklocal`
`no ipv6 eui64-linklocal`

Default The command **ipv6 eui64-linklocal** is enabled by default on any IPv6 enabled interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To enable IPv6 on an interface eth0, and use the link-local address of fe80::1/10 instead of the EUI-64 link-local that is automatically generated, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
awplus(config-if)# no ipv6 eui64-linklocal
awplus(config-if)# ipv6 address fe80::1/10
```

Related commands [ipv6 address](#)
[ipv6 address autoconfig](#)
[ipv6 enable](#)

Command changes Version 5.4.7-0.1: command added

ipv6 forwarding

Overview Use this command to turn on IPv6 unicast routing for IPv6 packet forwarding.

Use this command globally on your device before using the [ipv6 enable](#) command on individual interfaces.

Use the **no** variant of this command to turn off IPv6 unicast routing. Note IPv6 unicast routing is disabled by default.

Syntax `ipv6 forwarding`
`no ipv6 forwarding`

Mode Global Configuration

Default IPv6 unicast forwarding is disabled by default.

Usage notes Enable IPv6 unicast forwarding globally for all interfaces on your device with this command. Use the **no** variant of this command to disable IPv6 unicast forwarding globally for all interfaces on your device.

IPv6 unicast forwarding allows devices to communicate with devices that are more than one hop away, providing that there is a route to the destination address. If IPv6 forwarding is not enabled then pings to addresses on devices that are more than one hop away will fail, even if there is a route to the destination address.

Examples To enable IPv6 unicast routing, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
```

To disable IPv6 unicast routing, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 forwarding
```

Related commands [ipv6 enable](#)
[ipv6 multicast-routing](#)

ipv6 icmp error-interval

Overview Use this command to limit how often IPv6 ICMP error messages are sent. The maximum frequency of messages is specified in milliseconds.

Use the **no** variant of this command to reset the frequency to the default

Syntax `ipv6 icmp error-interval <interval>`
`no ipv6 icmp error-interval`

Parameter	Description
<interval>	0-2147483647, interval in milliseconds.

Default 1000

Mode Global Configuration

Example To configure the rate to be at most one packet every 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 icmp error-interval 10000
```

To reset the rate to the default of one packet every second, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 icmp error-interval
```

Related commands [ip icmp error-interval](#)

ipv6 multicast forward-slow-path-packet

Overview Use this command to enable multicast packets to be forwarded to the CPU. Enabling this command will ensure that the Layer 3 MTU is set correctly for each IP multicast group and will apply the value of the smallest MTU among the outgoing interfaces for the multicast group.

It will also ensure that a received packet that is larger than the MTU value will result in the generation of an ICMP Too Big message.

Use the **no** variant of this command to disable the above functionality.

Syntax `ipv6 multicast forward-slow-path-packet`
`no ipv6 multicast forward-slow-path-packet`

Default Disabled.

Mode Privileged Exec

Example To enable the ipv6 multicast forward-slow-path-packet function, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast forward-slow-path-packet
```

Related commands [show ipv6 forwarding](#)

Command changes Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

ipv6 multihoming

Overview Use this command to enable IPv6 multihoming. IPv6 multihoming dynamically adds IPv6 routes, with source prefixes, based on Neighbor Discovery Protocol (NDP) utilizing the Router Advertisements (RAs).

This allows segregation of traffic between multiple gateways, which is useful for sending traffic to multiple ISPs for increased redundancy and load balancing.

Use the **no** variant of this command to disable IPv6 multihoming.

Syntax `ipv6 multihoming`
`no ipv6 multihoming`

Default Disabled

Mode Interface Configuration

Usage notes Note that static IPv6 source address dependent routes do not require this feature.

Examples To configure IPv6 multihoming, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 multihoming
```

To disable IPv6 multihoming, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 multihoming
```

Related commands [ipv6 route](#)

Command changes Version 5.5.0-0.3: command added

ipv6 nd accept-ra-default-routes

Overview Use this command to allow accepting and installing of default routes based on a received RA (Router Advertisement). The default route's destination is set to the source address of the received RA.

Use the **no** variant of this command to disable accepting RA-based default routes.

Syntax `ipv6 nd accept-ra-default-routes`
`no ipv6 nd accept-ra-default-routes`

Default RA-based default routes are accepted by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To enable RA-based default routes on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd accept-ra-default-routes
```

Related commands [ipv6 address](#)
[ipv6 address autoconfig](#)
[ipv6 enable](#)

ipv6 nd accept-ra-pinfo

Overview Use this command to allow the processing of the prefix information included in a received RA (Router Advertisement) on an IPv6 enabled interface.

Use the **no** variant of this command to disable an IPv6 interface from using the prefix information within a received RA.

Syntax `ipv6 nd accept-ra-pinfo`
`no ipv6 nd accept-ra-pinfo`

Default The command **ipv6 nd accept-ra-pinfo** is enabled by default on any IPv6 interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes By default, when IPv6 is enabled on an interface, SLAAC is also enabled. SLAAC addressing along with the EUI-64 process, uses the prefix information included in a received RA to generate an automatic link-local address on the IPv6 interface.

Note: an AlliedWare Plus device will, by default, add a prefix for the connected interface IPv6 address(es) to the RA it transmits. However, this behavior can be changed by using the command **no ipv6 nd prefix auto-advertise**, so there is no guarantee that an RA will contain a prefix.

Example To enable IPv6 on eth0 without installing a SLAAC address on the interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
awplus(config-if)# no ipv6 nd accept-ra-pinfo
```

Related commands [ipv6 address](#)
[ipv6 address autoconfig](#)
[ipv6 enable](#)

Command changes Version 5.4.7-0.1: command added

ipv6 nd current-hoplimit

Overview Use this command to specify the advertised current hop limit used between IPv6 Routers.

Use the **no** variant of this command to reset the current advertised hop limit to the default of 0, which means no advertised current hop limit is specified.

Syntax `ipv6 nd current-hoplimit <hoplimit>`
`no ipv6 nd current-hoplimit`

Parameter	Description
<hoplimit>	Specifies the advertised current hop limit value. Valid values are from 0 to 255 hops.

Default 0 (No advertised current hop limit specified)

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Examples To set the advertised current hop limit to 2 between IPv6 Routers on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd current-hoplimit 2
```

To reset the advertised current hop limit to the default 0 on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd current-hoplimit
```

To set the advertised current hop limit to 2 between IPv6 Routers on ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd current-hoplimit 2
```

To reset the advertised current hop limit to the default 0 on ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 nd current-hoplimit
```

**Related
commands** [ipv6 nd managed-config-flag](#)
 [ipv6 nd prefix](#)
 [ipv6 nd suppress-ra](#)

ipv6 nd dns search-list

Overview Use this command to specify a DNS Search List (DNSSL) to be included in the Router Advertisement for a given IPv6 interface.

Use the **no** variant of this command to remove a specified domain name. If no domain name is specified, then all domain names previously added will be deleted.

Syntax `ipv6 nd dns search-list <domain-name>`
`no ipv6 nd dns search-list [<domain-name>]`

Parameter	Description
<code><domain-name></code>	A string specifying the domain name to be added to the search list. For example, myexample.com

Default No domain search list is included in router advertisements from any interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To add the domain name 'myexample.com' to the search list for eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd dns search-list myexample.com
```

To delete all domain names added previously, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd dns search-list
```

Related commands [ipv6 nd suppress-ra](#)

Command changes Version 5.5.0-2.5: command added

ipv6 nd dns-server

Overview Use this command to advertise (in Router Advertisement messages) a DNS server for downstream devices to use.

You can specify either a static IPv6 address or the lowest address from an interface.

Use the **no** variant of this command to delete one or all DNS server addresses.

Syntax `ipv6 nd dns-server {<int>|<ip-add>}`
`no ipv6 nd dns-server [<int>|<ip-add>]`

Parameter	Description
<int>	Advertise the lowest IPv6 address on the selected interface as a DNS server for downstream devices.
<ip-add>	Advertise a particular IPv6 address as a DNS server for downstream devices.

Default No DNS servers are advertised.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To configure eth0 to send RAs and advertise itself as a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd suppress-ra
awplus(config-if)# no ipv6 nd accept-ra-pinfo
awplus(config-if)# ipv6 address 2001:DB8::1/64
awplus(config-if)# ipv6 nd dns-server eth0
```

To configure eth0 to send RAs and advertise 2001:DB8::2 as a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd suppress-ra
awplus(config-if)# no ipv6 nd accept-ra-pinfo
awplus(config-if)# ipv6 address 2001:DB8::1/64
awplus(config-if)# ipv6 nd dns-server 2001:DB8::2
```

To stop advertising any DNS servers on the selected interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd dns-server
```

**Related
commands**

[ipv6 nd accept-ra-pinfo](#)
[ipv6 nd suppress-ra](#)
[show ipv6 interface](#)

ipv6 nd managed-config-flag

- Overview** Use this command to set the managed address configuration flag, contained within the router advertisement field.
- Setting this flag indicates the operation of a stateful autoconfiguration protocol such as DHCPv6 for address autoconfiguration, and that address information (i.e. the network prefix) and other (non-address) information can be requested from the device.
- An unset flag enables hosts receiving the advertisements to use a stateless autoconfiguration mechanism to establish their IPv6 addresses. The default is flag unset.
- Use the **no** variant of this command to reset this command to its default of having the flag unset.

Syntax `ipv6 nd managed-config-flag`
`no ipv6 nd managed-config-flag`

Default Unset

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes To enable the transmission of router advertisements, you must apply the **no** version of the [ipv6 nd suppress-ra](#) command. This step is included in the example below.

Example To set the managed address configuration flag on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd managed-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

To set the managed address configuration flag on the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd managed-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

Related commands [ipv6 nd suppress-ra](#)
[ipv6 nd prefix](#)
[ipv6 nd other-config-flag](#)

ipv6 nd minimum-ra-interval

Overview Use this command in Interface Configuration mode to set a minimum Router Advertisement (RA) interval for an interface.

Use the **no** variant of this command in Interface Configuration mode to remove the minimum RA interval for an interface.

Syntax `ipv6 nd minimum-ra-interval <seconds>`
`no ipv6 nd minimum-ra-interval`

Parameter	Description
<seconds>	Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 3 to 1350 seconds.

Default The RA interval for an interface is unset by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Examples To set the minimum RA interval for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd minimum-ra-interval 60
```

To remove the minimum RA interval for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd minimum-ra-interval
```

To set the minimum RA interval for the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd minimum-ra-interval 60
```

To remove the minimum RA interval for the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 nd minimum-ra-interval
```

**Related
commands**

- ipv6 nd ra-interval
- ipv6 nd suppress-ra
- ipv6 nd prefix
- ipv6 nd other-config-flag

ipv6 nd other-config-flag

Overview Use this command to set the **other** stateful configuration flag (contained within the router advertisement field) to be used for IPv6 address auto-configuration. This flag is used to request the router to provide information in addition to providing addresses.

Setting the [ipv6 nd managed-config-flag](#) command implies that the [ipv6 nd other-config-flag](#) will also be set.

Use **no** variant of this command to reset the value to the default.

Syntax `ipv6 nd other-config-flag`
`no ipv6 nd other-config-flag`

Default Unset

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes To enable the transmission of router advertisements, you must apply the **no** version of the [ipv6 nd suppress-ra](#) command. This step is included in the example below.

Example To set the IPv6 other-config-flag on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd other-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

To set the IPv6 other-config-flag on the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd other-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

Related commands [ipv6 nd suppress-ra](#)
[ipv6 nd prefix](#)
[ipv6 nd managed-config-flag](#)

ipv6 nd prefix

Overview Use this command in Interface Configuration mode to specify the IPv6 prefix information that is advertised by the router advertisement for IPv6 address auto-configuration.

Use the **no** parameter with this command to reset the IPv6 prefix for an interface in Interface Configuration mode.

Syntax

```
ipv6 nd prefix <ipv6-prefix/length>
ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime>
ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime>
<preferred-lifetime> [no-autoconfig]
ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime>
<preferred-lifetime> off-link [no-autoconfig]
no ipv6 nd prefix [<ipv6-addr/prefix-length>|all]
```

Parameter	Description
<ipv6-prefix/length>	The prefix to be advertised by the router advertisement message. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64. The default is X:X::/64.
<valid-lifetime>	The the period during which the specified IPv6 address prefix is valid. This can be set to a value between 0 and 4294967295 seconds. The default is 2592000 (30 days). Note that this period should be set to a value greater than that set for the prefix preferred-lifetime.
<preferred-lifetime>	Specifies the IPv6 prefix preferred lifetime. This is the period during which the IPv6 address prefix is considered a current (undeprecated) value. After this period, the command is still valid but should not be used in new communications. Set to a value between 0 and 4294967295 seconds. The default is 604800 seconds (7 days). Note that this period should be set to a value less than that set for the prefix valid-lifetime.
off-link	Specify the IPv6 prefix off-link flag. The default is flag set.
no-autoconfig	Specify the IPv6 prefix no autoconfiguration flag. Setting this flag indicates that the prefix is not to be used for autoconfiguration. The default is flag set.
all	Specify all IPv6 prefixes associated with the interface.

Default Valid-lifetime default is 2592000 seconds (30 days). Preferred-lifetime default is 604800 seconds (7 days).

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

Examples To configure the device to issue router advertisements on eth0, and advertise the address prefix of 2001:0db8::/64, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64
```

To configure the device to issue router advertisements on eth0, and advertise the address prefix of 2001:0db8::/64 with a valid lifetime of 10 days and a preferred lifetime of 5 days, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
```

To configure the device to issue router advertisements on eth0 and advertise the address prefix of 2001:0db8::/64 with a valid lifetime of 10 days, a preferred lifetime of 5 days, and no prefix used for autoconfiguration, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
no-autoconfig
```

To reset router advertisements on eth0, so the address prefix of 2001:0db8::/64 is not advertised from the device, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/64
```

To reset all router advertisements on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd prefix all
```

Related commands [ipv6 nd suppress-ra](#)

ipv6 nd proxy interface

Overview Use this command to enable the neighbor discovery proxy that forwards Neighbor Solicitations (NS) and Neighbor Advertisements (NA) between two interfaces.

Use the **no** variant of this command to disable the neighbor discovery proxy.

Syntax `ipv6 nd proxy interface <interface-name>`
`no ipv6 nd proxy`

Parameter	Description
<code><interface-name></code>	The name of the Ethernet or Bridge interface to proxy NS and NA from/to. For example eth1 or br1.

Default No ND proxy is enabled

Mode Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

Examples To enable neighbor discovery proxy on eth1, and forward NS and NA to eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 nd proxy interface eth0
```

To disable neighbor discovery proxy on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd proxy
```

Related commands [show running-config](#)

Command changes Version 5.4.8-1.1: command added

ipv6 nd ra-interval

Overview Use this command to specify the interval between IPv6 Router Advertisements (RA) transmissions.

Use **no** parameter with this command to reset the value to the default value (600 seconds).

Syntax `ipv6 nd ra-interval <seconds>`
`no ipv6 nd ra-interval`

Parameter	Description
<code><seconds></code>	Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 4 to 1800 seconds.

Default 600 seconds.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes To enable the transmission of router advertisements, you must apply the **no** version of the [ipv6 nd suppress-ra](#) command. This step is included in the example below.

Example To set the advertisements interval on eth0 to be 60 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd ra-interval 60
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the advertisements interval on eth0 to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd ra-interval
```

Related commands [ipv6 nd minimum-ra-interval](#)
[ipv6 nd suppress-ra](#)
[ipv6 nd prefix](#)

ipv6 nd ra-lifetime

Overview Use this command to specify the time period that this router can usefully act as a default gateway for the network. Each router advertisement resets this time period.

Use **no** parameter with this command to reset the value to default.

Syntax `ipv6 nd ra-lifetime <seconds>`
`no ipv6 nd ra-lifetime`

Parameter	Description
<seconds>	Time period in seconds. Valid values are from 0 to 9000. Note that you should set this time period to a value greater than the value you have set using the ipv6 nd ra-interval command.

Default 1800 seconds

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command specifies the lifetime of the current router to be announced in IPv6 Router Advertisements.

To enable the transmission of router advertisements, you must apply the **no** version of the [ipv6 nd suppress-ra](#) command. This step is included in the example below.

Examples To set the advertisement lifetime of 8000 seconds on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd ra-lifetime 8000
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the advertisement lifetime to the default on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd ra-lifetime
```

To set the advertisement lifetime of 8000 seconds on the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd ra-lifetime 8000
awplus(config-if)# no ipv6 nd suppress-ra
```

Related commands [ipv6 nd suppress-ra](#)
[ipv6 nd prefix](#)

ipv6 nd reachable-time

Overview Use this command to specify the reachable time in the router advertisement to be used for detecting reachability of the IPv6 neighbor.

Use the **no** variant of this command to reset the value to default.

Syntax `ipv6 nd reachable-time <milliseconds>`
`no ipv6 nd reachable-time`

Parameter	Description
<milliseconds>	Time period in milliseconds. Valid values are from 1000 to 3600000. Setting this value to 0 indicates an unspecified reachable-time.

Default 0 milliseconds

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command specifies the reachable time of the current router to be announced in IPv6 Router Advertisements.

To enable the transmission of router advertisements, you must apply the **no ipv6 nd suppress-ra** command. This instruction is included in the example shown below.

Example To set the reachable-time in router advertisements on eth0 to be 1800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd reachable-time 1800000
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the reachable-time in router advertisements on eth0 to an unspecified reachable-time (0 milliseconds), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd reachable-time
```

To set the reachable-time in router advertisements on the PPP interface ppp0 to be 1800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd reachable-time 1800000
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the reachable-time in router advertisements on the PPP interface ppp0 to an unspecified reachable-time (0 milliseconds), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 nd reachable-time
```

Related commands

- [ipv6 nd suppress-ra](#)
- [ipv6 nd prefix](#)

ipv6 nd retransmission-time

Overview Use this command to specify the advertised retransmission interval for Neighbor Solicitation in milliseconds between IPv6 Routers.

Use the **no** variant of this command to reset the retransmission time to the default (1 second).

Syntax `ipv6 nd retransmission-time <milliseconds>`
`no ipv6 nd retransmission-time`

Parameter	Description
<milliseconds>	Time period in milliseconds. Valid values are from 1000 to 3600000.

Default 1000 milliseconds (1 second)

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Examples To set the retransmission-time of Neighbor Solicitation on eth0 to be 800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd retransmission-time 800000
```

To reset the retransmission-time of Neighbor Solicitation on eth0 to the default 1000 milliseconds (1 second), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd retransmission-time
```

To set the retransmission-time of Neighbor Solicitation on the PPP interface ppp0 to be 800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 nd retransmission-time 800000
```

To reset the retransmission-time of Neighbor Solicitation on the PPP interface ppp0 to the default 1000 milliseconds (1 second), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 nd retransmission-time
```

**Related
commands** [ipv6 nd suppress-ra](#)
 [ipv6 nd prefix](#)

ipv6 nd route-information

Overview Use this command to supply more specific route information to be included in the RA (Router Advertisement) the device sends to downstream devices on the same link/LAN.

Use the **no** variant of this command to remove some or all route information.

Syntax

```
ipv6 nd route-information <ipv6-prefix/length>
[<0-4294967295>|infinity|default] [low|medium|high]

ipv6 nd route-information <ipv6-prefix/length>

no ipv6 nd route-information <ipv6-prefix/length>

no ipv6 nd route-information all
```

Parameter	Description
<ipv6-prefix/length>	The IPv6 network prefix and prefix length entered in dotted decimal format for the IPv6 network prefix, then slash notation for the IPv6 prefix length in the format X:X::X:X/ M, e.g. 2001:db8::/64
<0-4294967295> infinity default	The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for route determination. - infinity - specifies that the route advertisement has an infinite lifetime. - default - is 3 * MaxRtrAdvInterval
low medium high	The preference value for the route information

Default No route information option is included in router advertisement on any interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To configure a route of 2001:DB8:1::/48 on eth1.1, with a lifetime of 6000 seconds and a high preference, use the commands:

```
awplus# configure terminal
awplus(config)# int eth1.1
awplus(config-if)# ipv6 nd route-information 2001:DB8:1::/48
6000 high
```

Related commands [ipv6 nd suppress-ra](#)

Command changes Version 5.5.0-2.4: command added

ipv6 nd router-preference

Overview Use this command to set the default router preference in the router advertisements sent on a particular interface. You can use this setting to decide whether devices will use this router instead of an alternative router, by giving this router and the alternative router different values.

Use the **no** variant of this command to return the router preference to its default value.

Syntax `ipv6 nd router-preference {low|medium|high}`
`no ipv6 nd router-preference`

Parameter	Description
low	(0b11) Preference for this router on this interface is low.
medium	(0b00) Preference for this router on this interface is medium.
high	(0b01) Preference for this router on this interface is high.

Default Medium

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To set the router preference to high on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd router-preference high
```

Related commands [ipv6 nd suppress-ra](#)
[show ipv6 interface](#)

Command changes Version 5.5.1-0.1: command added

ipv6 nd suppress-ra

Overview Use this command to inhibit IPv6 Router Advertisement (RA) transmission for the current interface. Router advertisements are used when applying IPv6 stateless auto-configuration.

Use the **no** parameter with this command to enable Router Advertisement transmission.

Syntax `ipv6 nd suppress-ra`
`no ipv6 nd suppress-ra`

Default Router Advertisement (RA) transmission is suppressed by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Example To enable the transmission of router advertisements from eth0 on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd suppress-ra
```

To enable the transmission of router advertisements from ppp0 on the router, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 nd suppress-ra
```

Related commands [ipv6 nd ra-interval](#)
[ipv6 nd router-preference](#)
[ipv6 nd prefix](#)

ipv6 opportunistic-nd

Overview Use this command to enable opportunistic neighbor discovery for the global IPv6 ND cache. Opportunistic neighbor discovery changes the behavior for unsolicited ICMPv6 ND packet forwarding on the device.

Use the **no** variant of this command to disable opportunistic neighbor discovery for the global IPv6 ND cache.

Syntax `ipv6 opportunistic-nd`
`no ipv6 opportunistic-nd`

Default Opportunistic neighbor discovery is disabled by default.

Mode Global Configuration

Usage notes When opportunistic neighbor discovery is enabled, the device will reply to any received unsolicited ICMPv6 ND packets. The source MAC address for the unsolicited ICMPv6 ND packet is added to the IPv6 ND cache, so the device forwards the ICMPv6 ND packet. When opportunistic neighbor discovery is disabled, the source MAC address for the ICMPv6 packet is not added to the IPv6 ND cache, so the ICMPv6 ND packet is not forwarded by the device.

Examples To enable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# ipv6 opportunistic-nd
```

To disable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# no ipv6 opportunistic-nd
```

Related commands [arp opportunistic-nd](#)
[show ipv6 neighbors](#)
[show running-config interface](#)

ipv6 route

Overview This command adds a static IPv6 route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to forward packets and to advertise routes to neighbors.

The **no** variant of this command removes the static route.

Syntax `ipv6 route <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<src-prefix/length>] [<distvalue>] [description]`
`no ipv6 route <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<src-prefix/length>] [<distvalue>]`

Parameter	Description
<i><dest-prefix/length></i>	Specifies the destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<i><gateway-ip></i>	Specifies the address of the gateway (or next hop). The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<i><gateway-name></i>	Specifies the name of the interface for the gateway (or next hop).
<i><src-prefix/length></i>	Specifies the source prefix. This is used for SADR - see the Usage notes. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<i><distvalue></i>	Specifies the administrative distance for the route. Valid values are from 1 to 255. You can use administrative distance to determine which routes take priority over other routes. The route with the lowest distance value is used.
<i>description</i> <i><description></i>	A description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command show running-configuration .

Mode Global Configuration

Usage notes You can configure IPv6 static routes for Source Address Dependent Routing (SADR) by providing a source prefix. In 'normal' routing, when the device searches

routes for a next hop to forward a packet to, the device chooses the next hop based only on the destination address of the packet. When you provide SADR information for a route, the device also inspects the source address and ensures it fits within the source prefix range you provided for this route.

Versions of AlliedWare Plus earlier than 5.5.1-2.1 do not support descriptions on static routes, so a start-up configuration that contains descriptions will be rejected by these older versions. If you add descriptions, be careful if you downgrade to an older AlliedWare Plus version.

Example To create a route with administrative distance of 32 to send packets to 2001:0db8::1/128 via eth1.1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 32
```

To use SADR to create a route for packets from 2001::/64 to 2223::/64, with a next hop of 2001::1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2223::/64 2001::1 2001::/64
```

To give a route a description of 'test' when creating it, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 description
test
```

To remove the description from a route, re-enter the route without specifying the **description** parameter:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1
```

**Related
Commands** [ipv6 multihoming](#)
[show running-config](#)
[show ipv6 route](#)

**Command
changes** Version 5.5.1-2.1: **description** parameter added
Version 5.5.0-0.3: **src-prefix** parameter added

ipv6 unreachable

Overview Use this command to enable ICMPv6 (Internet Control Message Protocol version 6) type 1, destination unreachable, messages.

Use the **no** variant of this command to disable destination unreachable messages. This prevents an attacker from using these messages to discover the topology of a network.

Syntax `ipv6 unreachable`
`no ipv6 unreachable`

Default Destination unreachable messages are enabled by default.

Mode Global Configuration

Usage notes When a device receives a packet for a destination that is unreachable it returns an ICMPv6 type 1 message. This message includes a reason code, as per the table below. An attacker can use these messages to obtain information regarding the topology of a network. Disabling destination unreachable messages, using the **no ipv6 unreachable** command, secures your network against this type of probing.

NOTE: *Disabling ICMPv6 destination unreachable messages breaks applications such as traceroute, which depend on these messages to operate correctly.*

Table 18-1: ICMPv6 type 1 reason codes and description

Code	Description [RFC]
0	No route to destination [RFC4443]
1	Communication with destination administratively prohibited [RFC4443]
2	Beyond scope of source address [RFC4443]
3	Address unreachable [RFC4443]
4	Port unreachable [RFC4443]
5	Source address failed ingress/egress policy [RFC4443]
6	Reject route to destination [RFC4443]
7	Error in Source Routing Header [RFC6554]

Example To disable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# no ipv6 unreachable
```

To enable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# ipv6 unreachable
```

ping ipv6

Overview This command sends a query to another IPv6 host (send Echo Request messages).

Syntax `ping ipv6 {<host>|<ipv6-address>} [repeat
{<1-2147483647>|continuous}] [size <10-1452>] [interface
<interface-list>] [timeout <1-65535>]`

Parameter	Description
<ipv6-addr>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<hostname>	The destination hostname.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
size <10-1452>	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
interface <interface-list>	The interface or range of configured IP interfaces to use as the source in the IP header of the ping packet. The interface can be one of: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. You can only specify the interface when pinging a link local address.
timeout <1-65535>	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
continuous	Continuous ping.

Parameter	Description
size <10-1452>	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
timeout <1-65535>	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.

Mode User Exec and Privileged Exec

Example awplus# ping ipv6 2001:0db8::a2

Related commands [traceroute ipv6](#)

show ipv6 forwarding

Overview Use this command to display IPv6 forwarding status.

Syntax `show ipv6 forwarding`

Mode User Exec and Privileged Exec

Example `awplus# show ipv6 forwarding`

Output Figure 18-1: Example output from the **show ipv6 forwarding** command

```
awplus#show ipv6 forwarding
ipv6 forwarding is on
```

show ipv6 interface

Overview Use this command to display brief information about interfaces and the IPv6 address assigned to them.

Syntax `show ipv6 interface [brief|<interface-list>] [nd]`

Parameter	Description
brief	Specify this optional parameter to display brief IPv6 interface information.
<interface-list>	The interfaces to display information about. An interface-list can be: - a PPP interface (e.g. ppp0) - an Eth interface (e.g. eth0) - an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. - a bridge interface (e.g. br0) - a tunnel interface (e.g. tunnel0) - the loopback interface (lo) - a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) - a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. The specified interfaces must exist.
nd	Specify this optional parameter for Neighbor Discovery configurations.

Mode User Exec and Privileged Exec

Examples To display a brief list of all interfaces on a device, use the following command:

```
awplus# show ipv6 interface brief
```

Output Figure 18-2: Example output from the **show ipv6 interface brief** command

awplus#show ipv6 interface brief			
Interface	IPv6-Address	Status	Protocol
eth1	unassigned	admin up	running
eth1.1	2001:db8::1/48	admin up	down
	fe80::215:77ff:fee9:5c50/64		
lo	unassigned	admin up	running

Related commands [ipv6 nd router-preference](#)
[show interface brief](#)

show ipv6 neighbors

Overview Use this command to display all IPv6 neighbors.

For information on filtering and saving command output, see the [“Getting_Started with AlliedWare Plus” Feature Overview and Configuration_Guide](#).

Syntax `show ipv6 neighbors`

Mode User Exec and Privileged Exec

Example To display a device’s IPv6 neighbors, use the following command:

```
awplus# show ipv6 neighbors
```

Output Figure 18-3: Example output of the **show ipv6 neighbors** command

IPv6 Address	MAC Address	Interface	Port	Type
fe80::290:bff:fe3e:44dc	0090.0b3e.44dc	eth1	-	dynamic
fd32:b1f0:ddf7:ab03::1	0090.0b3e.44dc	eth1	-	dynamic
...				

Related commands [clear ipv6 neighbors](#)

show ipv6 route

Overview Use this command to display the IPv6 routing table for a protocol or from a particular table.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 route`
`[bgp|connected|database|ospf|rip|static|summary|<ipv6-address>`
`|<ipv6-prefix/prefix-length>]`

Parameter	Description
bgp	Displays only the routes learned from BGP.
connected	Displays only the routes learned from connected interfaces.
database	Displays only the IPv6 routing information extracted from the database.
ospf	Displays only the routes learned from OSPFv3.
rip	Displays only the routes learned from RIPng.
static	Displays only the IPv6 static routes you have configured.
summary	Displays summary information from the IPv6 routing table.
<ipv6-address>	Displays the routes for the specified address in the IPv6 routing table.
<ipv6-prefix>/<prefix-length>	Displays only the routes for the specified IPv6 prefix.

Mode User Exec and Privileged Exec

Example To display all IPv6 routes with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

To display all database entries for all IPv6 routes, use the following command:

```
awplus# show ipv6 route database
```

Output Figure 18-4: Example output of the **show ipv6 route** command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
S   ::/0 [1/0] via 2001::a:0:0:c0a8:a6, eth1
C   2001:db8::a:0:0:0/64 via ::, eth1
...
```

Output Figure 18-5: Example output of the **show ipv6 route database** command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
> - selected route, * - FIB route, p - stale info
Timers: Uptime

S    ::/0 [1/0] via 2001::a:0:0:c0a8:a01 inactive, 6d22h12m
      [1/0] via 2001::fa:0:0:c0a8:fa01 inactive, 6d22h12m
```

show ipv6 route summary

Overview Use this command to display the summary of the current NSM RIB entries.
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 route summary`

Mode User Exec and Privileged Exec

Example To display IP route summary, use the following command:

```
awplus# show ipv6 route summary
```

Output Figure 18-6: Example output from the **show ipv6 route summary** command

IPv6 routing table name is Default-IPv6-Routing-Table(0)	
IPv6 routing table maximum-paths is 4	
RouteSource	Networks
connected	4
rip	5
Total	9
FIB	5

Related commands [show ip route database](#)

traceroute ipv6

Overview Use this command to trace the route to the specified IPv6 host.

Syntax `traceroute ipv6 {<ipv6-addr>|<hostname>}`

Parameter	Description
<code><ipv6-addr></code>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<code><hostname></code>	The destination hostname.

Mode User Exec and Privileged Exec

Example To run a traceroute for the IPv6 address 2001:0db8::a2, use the following command:

```
awplus# traceroute ipv6 2001:0db8::a2
```

Related commands [ping ipv6](#)

19

Routing Commands

Introduction

Overview This chapter provides an alphabetical reference of routing commands that are common across the routing IP protocols. For more information, see the [Route Selection Feature Overview and Configuration Guide](#).

- Command List**
- ["ip resolve-via-default"](#) on page 622
 - ["ip route"](#) on page 623
 - ["ipv6 route"](#) on page 626
 - ["max-fib-routes"](#) on page 628
 - ["max-static-routes"](#) on page 629
 - ["maximum-paths"](#) on page 630
 - ["show ip resolve-via-default"](#) on page 631
 - ["show ip route"](#) on page 632
 - ["show ip route database"](#) on page 635
 - ["show ip route summary"](#) on page 637
 - ["show ipv6 route"](#) on page 638
 - ["show ipv6 route summary"](#) on page 640

ip resolve-via-default

Overview Use this command to enable a routing protocol (most likely BGP) to use a default route to resolve next hops.

This command affects recursive routes, which are routes where the next hop is defined in terms of another IP address, and therefore resolving the next hop requires another route lookup. Recursive routes are most common in BGP but can occur in other routing protocols too.

Use the **no** variant of this command to stop the protocol from using a default route to resolve next hops. This can be helpful when such use can lead to inappropriate next hops being incorrectly activated.

Syntax `ip resolve-via-default`
`no ip resolve-via-default`

Default Enabled

Mode Global Configuration

Usage notes This command's effect is not instantaneous. Changing this setting does not result in an recalculation of all routes. Instead, the command will only result in changes when routes are recalculated, or if you manually restart the routing protocol.

Example To stop the device from using default routes to resolve next hops, use the commands:

```
awplus# configure terminal
awplus(config)# no ip resolve-via-default
```

To allow the device to use default routes to resolve next hops again, use the commands:

```
awplus# configure terminal
awplus(config)# ip resolve-via-default
```

Related commands [show ip resolve-via-default](#)

Command changes Version 5.5.3-0.1: command added

ip route

Overview This command adds a static route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to advertise routes to neighbors and forward packets.

The **no** variant of this command removes the static route from the RIB and FIB.

Syntax `ip route <subnet&mask> {<gateway-ip>|<interface>} [<distance>]
[weight <1-255>] [description <description>]
no ip route <subnet&mask> {<gateway-ip>|<interface>}
[<distance>] [weight <1-255>]`

Parameter	Description
<subnet&mask>	The IPv4 address of the destination subnet defined using either a prefix length or a separate mask specified in one of the following formats: - The IPv4 subnet address in dotted decimal notation followed by the subnet mask, also in dotted decimal notation. - The IPv4 subnet address in dotted decimal notation, followed by a forward slash, then the prefix length.
<gateway-ip>	The IPv4 address of the gateway device.
<interface>	The interface that connects your device to the network. You can also enter 'null' as an interface. Specify a 'null' interface to add a null or blackhole route to the device. The gateway IP address or the interface is required.
<distance>	The administrative distance for the static route in the range 1 to 255. Static routes by default have an administrative distance of 1, which gives them the highest priority possible.
weight <1-255>	Weight is used for the Weighted Lottery Load Balancing mode. See the Usage notes section for more information.
description <description>	A description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command show running-configuration .

Mode Global Configuration

Default The default administrative distance for a static route is 1.

Usage notes You can use administrative distance to determine which routes take priority over other routes.

Specify a 'Null' interface to add a null or blackhole route to the switch. A null or blackhole route is a routing table entry that does not forward packets, so any packets sent to it are dropped.

Versions of AlliedWare Plus earlier than 5.5.1-2.1 do not support descriptions on static routes, so a start-up configuration that contains descriptions will be rejected by these older versions. If you add descriptions, be careful if you downgrade to an older AlliedWare Plus version.

The **weight** parameter lets you assign a weight to the interface. AlliedWare Plus distributes the work load based on the number of sessions that are connected through the interfaces. It uses the weight that you assign to each interface to calculate a percentage of the total sessions that are allowed to connect through each interface. It then distributes the number of sessions between the interfaces accordingly.

Examples To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at 10.10.0.2 with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To remove the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at 10.10.0.2 with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# no ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To specify a null or blackhole route 192.168.4.0/24, so packets forwarded to this route are dropped, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.4.0/24 null
```

To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at 10.10.0.2 with an administrative distance of 128, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
128
```

To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at 10.10.0.2 with the default administrative distance, and a weight of 7, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
weight 7
```

To give a route a description of 'test' when creating it, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0/24 10.10.0.2 description
test
```

To remove the description from a route, re-enter the route without specifying the **description** parameter:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0/24 10.10.0.2
```

**Related
commands**

[show ip route](#)
[show ip route database](#)

**Command
changes**

Version 5.5.1-2.1: **weight** and **description** parameters added.
Version 5.5.2-2.1: **weight** parameter added for 10GbE UTM firewall.

ipv6 route

Overview This command adds a static IPv6 route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to forward packets and to advertise routes to neighbors.

The **no** variant of this command removes the static route.

Syntax `ipv6 route <dest-prefix/length> {<gateway-ip>|<gateway-name>} [<src-prefix/length>] [<distvalue>] [description]`
`<description>`
`no ipv6 route <dest-prefix/length>`
`{<gateway-ip>|<gateway-name>} [<src-prefix/length>] [<distvalue>]`

Parameter	Description
<i><dest-prefix/length></i>	Specifies the destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<i><gateway-ip></i>	Specifies the address of the gateway (or next hop). The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<i><gateway-name></i>	Specifies the name of the interface for the gateway (or next hop).
<i><src-prefix/length></i>	Specifies the source prefix. This is used for SADR - see the Usage notes. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<i><distvalue></i>	Specifies the administrative distance for the route. Valid values are from 1 to 255. You can use administrative distance to determine which routes take priority over other routes. The route with the lowest distance value is used.
description <i><description></i>	A description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command show running-configuration .

Mode Global Configuration

Usage notes You can configure IPv6 static routes for Source Address Dependent Routing (SADR) by providing a source prefix. In 'normal' routing, when the device searches

routes for a next hop to forward a packet to, the device chooses the next hop based only on the destination address of the packet. When you provide SADR information for a route, the device also inspects the source address and ensures it fits within the source prefix range you provided for this route.

Versions of AlliedWare Plus earlier than 5.5.1-2.1 do not support descriptions on static routes, so a start-up configuration that contains descriptions will be rejected by these older versions. If you add descriptions, be careful if you downgrade to an older AlliedWare Plus version.

Example To create a route with administrative distance of 32 to send packets to 2001:0db8::1/128 via eth1.1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 32
```

To use SADR to create a route for packets from 2001::/64 to 2223::/64, with a next hop of 2001::1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2223::/64 2001::1 2001::/64
```

To give a route a description of 'test' when creating it, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 description
test
```

To remove the description from a route, re-enter the route without specifying the **description** parameter:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1
```

**Related
Commands** [ipv6 multihoming](#)
[show running-config](#)
[show ipv6 route](#)

**Command
changes** Version 5.5.1-2.1: **description** parameter added
Version 5.5.0-0.3: **src-prefix** parameter added

max-fib-routes

Overview This command enables you to control the maximum number of FIB routes configured. It operates by providing parameters that enable you to configure preset maximums and warning message thresholds.

NOTE: For static routes use the [max-static-routes](#) command.

Use the **no** variant of this command to set the maximum number of FIB routes to the default of 4294967294 FIB routes.

Syntax `max-fib-routes <1-4294967294> [<1-100>|warning-only]`
`no max-fib-routes`

Parameter	Description
<code>max-fib-routes</code>	This is the maximum number of routes that can be stored in the device's Forwarding Information dataBase. In practice, other practical system limits would prevent this maximum being reached.
<code><1-4294967294></code>	The allowable configurable range for setting the maximum number of FIB-routes.
<code><1-100></code>	This parameter enables you to optionally apply a percentage value. This percentage will be based on the maximum number of FIB routes you have specified. This will cause a warning message to appear when your routes reach your specified percentage value. Routes can continue to be added until your configured maximum value is reached.
<code>warning-only</code>	This parameter enables you to optionally apply a warning message. If you set this option a warning message will appear if your maximum configured value is reached. Routes can continue to be added until your device reaches either the maximum capacity value of 4294967294, or a practical system limit.

Default The default number of FIB routes is the maximum number of FIB routes (4294967294).

Mode Global Configuration

Examples To set the maximum number of dynamic routes to 2000 and warning threshold of 75%, use the following commands:

```
awplus# config terminal
awplus(config)# max-fib-routes 2000 75
```


max-static-routes

Overview Use this command to set the maximum number of static routes, excluding FIB (Forwarding Information Base) routes.

NOTE: For FIB routes use the [max-fib-routes](#) command.

Use the **no** variant of this command to set the maximum number of static routes to the default of 1024 static routes.

Syntax `max-static-routes <1-1024>`
`no max-static-routes`

Default The default number of static routes is the maximum number of static routes (1024).

Mode Global Configuration

Example To reset the maximum number of static routes to the default maximum, use the command:

```
awplus# configure terminal
awplus(config)# no max-static-routes
```

NOTE: Static routes are applied before adding routes to the RIB (Routing Information Base). Therefore, rejected static routes will not appear in the running config.

Related commands [max-fib-routes](#)

maximum-paths

Overview This command enables ECMP on your device, and sets the maximum number of paths that each route has in the Forwarding Information Base (FIB). ECMP is enabled by default.

The **no** variant of this command sets the maximum paths to the default of 4.

ECMP path calculations are flow-based. This means that packets from the same flow will always be sent on the same path.

Syntax `maximum-paths <1-8>`
`no maximum-paths`

Parameter	Description
<1-8>	The maximum number of paths that a route can have in the FIB.

Default By default the maximum number of paths is 4.

Mode Global Configuration

Examples To set the maximum number of paths for each route in the FIB to 5, use the commands:

```
awplus# configure terminal
awplus(config)# maximum-paths 5
```

To set the maximum paths for a route to the default of 4, use the commands:

```
awplus# configure terminal
awplus(config)# no maximum-paths
```

Command changes Version 5.5.2-2.2: command added to x330 and GS970EMX series

show ip resolve-via-default

Overview Use this command to see whether it is possible to use a default route to resolve next hops in IP routing. By default it is possible, but this can be changed with the **no** variant of the command [ip resolve-via-default](#).

Syntax `show ip resolve-via-default`

Mode User Exec

Example To show whether default routes are used to resolve next hops or not, use the command:

```
awplus# show ip resolve-via-default
```

Output Figure 19-1: Example output from **show ip resolve-via-default**:

```
awplus#show ip resolve-via-default
IP resolve via default is off
```

Related commands [ip resolve-via-default](#)

Command changes Version 5.5.3-0.1: command added

show ip route

Overview Use this command to display routing entries in the FIB (Forwarding Information Base). The FIB contains the best routes to a destination, and your device uses these routes when forwarding traffic. You can display a subset of the entries in the FIB based on protocol.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token.

Syntax `show ip route [bgp|connected|ospf|rip|static|
<ip-addr>|<ip-addr/prefix-length>]`

Parameter	Description
bgp	Displays only the routes learned from BGP.
connected	Displays only the routes learned from connected interfaces.
ospf	Displays only the routes learned from OSPF.
rip	Displays only the routes learned from RIP.
static	Displays only the static routes you have configured.
<ip-addr>	Displays the routes for the specified address. Enter an IPv4 address.
<ip-addr/prefix-length>	Displays the routes for the specified network. Enter an IPv4 address and prefix length.

Mode User Exec and Privileged Exec

Examples To display the static routes in the FIB, use the command:

```
awplus# show ip route static
```

To display the OSPF routes in the FIB, use the command:

```
awplus# show ip route ospf
```

Output Each entry in the output from this command has a code preceding it, indicating the source of the routing entry. For example, O indicates OSPF as the origin of the route. The first few lines of the output list the possible codes that may be seen with the route entries.

Typically, route entries are composed of the following elements:

- code
- a second label indicating the sub-type of the route
- network or host IP address
- administrative distance and metric

- next hop IP address
- outgoing interface name
- time since route entry was added

Figure 19-2: Example output from the **show ip route** command

```
awplus#show ip route
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, D - DHCP, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default

Gateway of last resort is 10.37.227.65 to network 0.0.0.0

S      10.32.18.135/32 [1/0] via 10.37.163.129, eth1
S      10.33.0.0/16 [1/0] via 10.37.163.129, eth1
C      10.37.163.128/27 is directly connected, eth1
...
```

Connected Route An example of a connected route entry consists of:

```
C      10.10.31.0/24 is directly connected, eth1
```

This route entry denotes:

- Route entries for network 10.10.31.0/24 are derived from the IP address of local interface eth1.
- These routes are marked as Connected routes (C) and always preferred over routes for the same network learned from other routing protocols.

OSPF Route An example of an OSPF route entry consists of:

```
O      10.10.37.0/24 [110/11] via 10.10.31.16, eth1, 00:20:54
```

This route entry denotes:

- This route in the network 10.10.37.0/24 was added by OSPF.
- This route has an administrative distance of 110 and metric/cost of 11.
- This route is reachable via next hop 10.10.31.16.
- The outgoing local interface for this route is eth1.
- This route was added 20 minutes and 54 seconds ago.

OSPF External Route An example of an OSPF external route entry consists of:

```
O E2   14.5.1.0/24 [110/20] via 10.10.31.16, eth1, 00:18:56
```

This route entry denotes that this route is the same as the other OSPF route explained above; the main difference is that it is a Type 2 External OSPF route.

Weight for Static Route If the **weight** parameter has been set using the **ip route** command, it will be shown in the output:

```
S      10.10.37.0/24 [110/11] via 10.10.31.16, eth1 weight 5
                                via 10.10.31.32, eth1 weight 1
```

AlliedWare Plus distributes the work load based on the number of sessions that are connected through the interfaces. It uses the weight that you assign to each interface to calculate a percentage of the total sessions that are allowed to connect through each interface. It then distributes the number of sessions between the interfaces accordingly.

Related commands [ip route](#)
[maximum-paths](#)
[show ip route database](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

show ip route database

Overview This command displays the routing entries in the RIB (Routing Information Base).

When multiple entries are available for the same prefix, RIB uses the routes' administrative distances to choose the best route. All best routes are entered into the FIB (Forwarding Information Base). To view the routes in the FIB, use the [show ip route](#) command.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token).

Syntax `show ip route database [bgp|connected|ospf|rip|static]`

Parameter	Description
bgp	Displays only the routes learned from BGP.
connected	Displays only the routes learned from connected interfaces.
ospf	Displays only the routes learned from OSPF.
rip	Displays only the routes learned from RIP.
static	Displays only the static routes you have configured.

Mode User Exec and Privileged Exec

Example To display the static routes in the RIB, use the command:

```
awplus# show ip route database static
```

Output Figure 19-3: Example output from the **show ip route database** command:

```
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       > - selected route, * - FIB route, p - stale info

O    *> 9.9.9.9/32 [110/31] via 10.10.31.16, eth1, 00:19:21
O    10.10.31.0/24 [110/1] is directly connected, eth1, 00:28:20
C    *> 10.10.31.0/24 is directly connected, eth1
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, eth1
O    10.10.34.0/24 [110/31] via 10.10.31.16, eth1, 00:21:19
O    *> 10.10.37.0/24 [110/11] via 10.10.31.16, eth1, 00:21:19
C    *> 10.30.0.0/24 is directly connected, eth1
S    *> 11.22.11.0/24 [1/0] via 10.10.31.16, eth1
O E2 *> 14.5.1.0/24 [110/20] via 10.10.31.16,eth1, 00:19:21
O    16.16.16.16/32 [110/11] via 10.10.31.16, eth1, 00:21:19
S    *> 16.16.16.16/32 [1/0] via 10.10.31.16, eth1
O    *> 17.17.17.17/32 [110/31] via 10.10.31.16, eth1, 00:21:19
C    *> 45.45.45.45/32 is directly connected, lo
O    *> 55.55.55.55/32 [110/21] via 10.10.31.16, eth1, 00:21:19
C    *> 127.0.0.0/8 is directly connected, lo
```

Related commands [maximum-paths](#)
[show ip route](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

show ip route summary

Overview This command displays a summary of the current RIB (Routing Information Base) entries.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token.

Syntax `show ip route summary`

Mode User Exec and Privileged Exec

Example To display a summary of the current RIB entries, use the command:

```
awplus# show ip route summary
```

Output Figure 19-4: Example output from the **show ip route summary** command

```
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source      Networks
connected         5
ospf               2
Total             8
```

Related commands [show ip route](#)
[show ip route database](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

show ipv6 route

Overview Use this command to display the IPv6 routing table for a protocol or from a particular table.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 route`
`[bgp|connected|database|ospf|rip|static|summary|<ipv6-address>`
`|<ipv6-prefix/prefix-length>]`

Parameter	Description
bgp	Displays only the routes learned from BGP.
connected	Displays only the routes learned from connected interfaces.
database	Displays only the IPv6 routing information extracted from the database.
ospf	Displays only the routes learned from OSPFv3.
rip	Displays only the routes learned from RIPng.
static	Displays only the IPv6 static routes you have configured.
summary	Displays summary information from the IPv6 routing table.
<ipv6-address>	Displays the routes for the specified address in the IPv6 routing table.
<ipv6-prefix>/<prefix-length>	Displays only the routes for the specified IPv6 prefix.

Mode User Exec and Privileged Exec

Example To display all IPv6 routes with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

To display all database entries for all IPv6 routes, use the following command:

```
awplus# show ipv6 route database
```

Output Figure 19-5: Example output of the **show ipv6 route** command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
S   ::/0 [1/0] via 2001::a:0:0:c0a8:a6, eth1
C   2001:db8::a:0:0:0/64 via ::, eth1
...
```

Output Figure 19-6: Example output of the **show ipv6 route database** command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
> - selected route, * - FIB route, p - stale info
Timers: Uptime

S   ::/0 [1/0] via 2001::a:0:0:c0a8:a01 inactive, 6d22h12m
      [1/0] via 2001::fa:0:0:c0a8:fa01 inactive, 6d22h12m
```

show ipv6 route summary

Overview Use this command to display the summary of the current NSM RIB entries.
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 route summary`

Mode User Exec and Privileged Exec

Example To display IP route summary, use the following command:

```
awplus# show ipv6 route summary
```

Output Figure 19-7: Example output from the **show ipv6 route summary** command

IPv6 routing table name is Default-IPv6-Routing-Table(0)	
IPv6 routing table maximum-paths is 4	
RouteSource	Networks
connected	4
rip	5
Total	9
FIB	5

Related commands [show ip route database](#)

20

RIP Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure RIP.

For information about configuring RIP, see the [RIP Feature Overview and Configuration Guide](#).

- Command List**
- ["accept-lifetime"](#) on page 643
 - ["alliedware-behavior"](#) on page 645
 - ["cisco-metric-behavior \(RIP\)"](#) on page 647
 - ["clear ip rip route"](#) on page 648
 - ["debug rip"](#) on page 649
 - ["default-information originate \(RIP\)"](#) on page 650
 - ["default-metric \(RIP\)"](#) on page 651
 - ["distance \(RIP\)"](#) on page 652
 - ["distribute-list \(RIP\)"](#) on page 653
 - ["fullupdate \(RIP\)"](#) on page 654
 - ["ip summary-address rip"](#) on page 655
 - ["ip prefix-list"](#) on page 656
 - ["ip rip authentication key-chain"](#) on page 658
 - ["ip rip authentication mode"](#) on page 660
 - ["ip rip authentication string"](#) on page 662
 - ["ip rip receive-packet"](#) on page 664
 - ["ip rip receive version"](#) on page 665
 - ["ip rip send-packet"](#) on page 666

- ["ip rip send version"](#) on page 667
- ["ip rip send version 1-compatible"](#) on page 669
- ["ip rip split-horizon"](#) on page 670
- ["key"](#) on page 671
- ["key chain"](#) on page 672
- ["key-string"](#) on page 673
- ["maximum-prefix"](#) on page 674
- ["neighbor \(RIP\)"](#) on page 675
- ["network \(RIP\)"](#) on page 676
- ["passive-interface \(RIP\)"](#) on page 677
- ["recv-buffer-size \(RIP\)"](#) on page 678
- ["redistribute \(RIP\)"](#) on page 679
- ["restart rip graceful"](#) on page 680
- ["rip restart grace-period"](#) on page 681
- ["route \(RIP\)"](#) on page 682
- ["router rip"](#) on page 683
- ["send-lifetime"](#) on page 684
- ["show debugging rip"](#) on page 686
- ["show ip prefix-list"](#) on page 687
- ["show ip protocols rip"](#) on page 688
- ["show ip rip"](#) on page 689
- ["show ip rip database"](#) on page 690
- ["show ip rip interface"](#) on page 691
- ["timers \(RIP\)"](#) on page 692
- ["undebg rip"](#) on page 694
- ["version \(RIP\)"](#) on page 695

accept-lifetime

Overview Use this command to specify the time period during which the authentication key on a key chain is received as valid.

Use the **no** variant of this command to remove a specified time period for an authentication key on a key chain as set previously with the **accept-lifetime** command.

Syntax `accept-lifetime <start-date> {<end-date>|
duration <seconds>|infinite}
no accept-lifetime`

Parameter	Description
<start-date>	Specifies the start time and date in the format: <hh:mm:ss> <day> <month> <year> or <hh:mm:ss> <month> <day> <year>, where:
	<hh:mm:ss> The time of the day, in hours, minutes and seconds
	<day> <1-31> The day of the month
	<month> The month of the year (the first three letters of the month, for example, Jan)
	<year> <1993-2035> The year
<end-date>	Specifies the end time and date in the format: <hh:mm:ss> <day> <month> <year> or <hh:mm:ss> <month> <day> <year>, where:
	<hh:mm:ss> The time of the day, in hours, minutes and seconds
	<day> <1-31> The day of the month
	<month> The month of the year (the first three letters of the month, for example, Jan)
	<year> <1993-2035> The year
<seconds>	<1-2147483646> Duration of the key in seconds.
infinite	Never expires.

Mode Keychain-key Configuration

Examples The following examples show the setting of accept-lifetime for key 1 on the key chain named "mychain".

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# accept-lifetime 03:03:01 Sep 3
2016 04:04:02 Oct 6 2016
```

or:

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# accept-lifetime 03:03:01 3 Sep
2016 04:04:02 6 Oct 2016
```

**Related
commands**

[key](#)
[key-string](#)
[key chain](#)
[send-lifetime](#)

alliedware-behavior

Overview This command configures your device to exhibit AlliedWare behavior when sending RIPv1 response/update messages. Configuring for this behavior may be necessary if you are replacing an AlliedWare device with an AlliedWare Plus device and wish to ensure consistent RIPv1 behavior.

Use the **no** variant of this command to implement AlliedWare Plus behavior.

This command has no impact on devices running RIPv2. Reception and transmission can be independently altered to conform to AlliedWare standard.

Syntax `alliedware-behavior {rip1-send|rip1-recv}`
`no alliedware-behavior {rip1-send|rip1-recv}`

Parameter	Description
<code>rip1-send</code>	Configures the router to behave in AlliedWare mode when sending update messages.
<code>rip1-recv</code>	Configures the router to behave in AlliedWare mode when receiving update messages.

Default By default when sending out RIPv1 updates on an interface, if the prefix (learned through RIPv2 or otherwise redistributed into RIP) being advertised does not match the subnetting used on the outgoing RIPv1 interface it will be filtered. The **alliedware-behavior** command returns your router's RIPv1 behavior to the AlliedWare format, where the prefix will be advertised as-is.

For example, if a RIPv1 update is being sent over interface 192.168.1.4/26, by default the prefix 192.168.1.64/26 will be advertised, but the prefix 192.168.1.144/28 will be filtered because the mask /28 does not match the interface's mask of /26. If **alliedware-behavior rip1-send** is configured, 192.168.1.144 would be sent as-is.

Mode Router Configuration

Examples To configure your device for **AlliedWare**-like behavior when sending and receiving RIPv1 update messages, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# alliedware-behavior rip1-send
awplus(config-router)# alliedware-behavior rip1-recv
```

To return your device to **AlliedWare Plus**-like behavior when sending and receiving RIPv1 update messages, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no alliedware-behavior rip1-send
awplus(config-router)# no alliedware-behavior rip1-recv
```

**Validation
Commands** [show ip protocols rip](#)
 [show running-config](#)

**Related
commands** [fullupdate \(RIP\)](#)

cisco-metric-behavior (RIP)

Overview Use this command to enable or disable the RIP routing metric update to conform to Cisco's implementation. This command is provided to allow inter-operation with older Cisco devices that do not conform to the RFC standard for RIP route metrics.

Use the **no** variant of this command to disable this feature.

Syntax `cisco-metric-behavior {enable|disable}`
`no cisco-metric-behavior`

Parameter	Description
enable	Enables updating the metric consistent with Cisco.
disable	Disables updating the metric consistent with Cisco.

Default By default, the Cisco metric-behavior is disabled.

Mode Router Configuration

Examples To enable the routing metric update to behave as per the Cisco implementation, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# cisco-metric-behavior enable
```

To disable the routing metric update to behave as per the default setting, enter the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no cisco-metric-behavior
```

Validation Commands `show running-config`

clear ip rip route

Overview Use this command to clear specific data from the RIP routing table.

Syntax `clear ip rip route <ip-dest-network/prefix-length>`
`clear ip rip route`
`{static|connected|rip|ospf|bgp|invalid-routes|all}`

Parameter	Description
<code><ip-dest-network/prefix-length></code>	Removes entries which exactly match this destination address from RIP routing table. Enter the IP address and prefix length of the destination network.
<code>static</code>	Removes static entries from the RIP routing table.
<code>connected</code>	Removes entries for connected routes from the RIP routing table.
<code>rip</code>	Removes only RIP routes from the RIP routing table.
<code>ospf</code>	Removes only OSPF routes from the RIP routing table.
<code>bgp</code>	Removes only BGP routes from the RIP routing table.
<code>invalid-routes</code>	Removes routes with metric 16 immediately. Otherwise, these routes are not removed until RIP times out the route after 2 minutes.
<code>all</code>	Clears the entire RIP routing table.

Mode Privileged Exec

Usage notes Using this command with the **all** parameter clears the RIP table of all the routes.

Examples To clear the route 10.0.0.0/8 from the RIP routing table, use the following command:

```
awplus# clear ip rip route 10.0.0.0/8
```

debug rip

Overview Use this command to specify the options for the displayed debugging information for RIP events and RIP packets.

Use the **no** variant of this command to disable the specified debug option.

Syntax `debug rip {events|nsm|<packet>|all}`
`no debug rip {events|nsm|<packet>|all}`

Parameter	Description
events	RIP events debug information is displayed.
nsm	RIP and NSM communication is displayed.
<packet>	packet [recv send] [detail] Specifies RIP packets only.
recv	Specifies that information for received packets be displayed.
send	Specifies that information for sent packets be displayed.
detail	Displays detailed information for the sent or received packet.
all	Displays all RIP debug information.

Default Disabled

Mode Privileged Exec and Global Configuration

Example The following example displays information about the RIP packets that are received and sent out from the device.

```
awplus# debug rip packet
```

Related commands [undebug rip](#)

default-information originate (RIP)

Overview Use this command to generate a default route into the Routing Information Protocol (RIP).

Use the **no** variant of this command to disable this feature.

Syntax `default-information originate`
`no default-information originate`

Default Disabled

Mode Router Configuration

Usage If routes are being redistributed into RIP and the router's route table contains a default route, within one of the route categories that are being redistributed, the RIP protocol will advertise this default route, irrespective of whether the **default-information originate** command has been configured or not. However, if the router has not redistributed any default route into RIP, but you want RIP to advertise a default route anyway, then use this command.

This will cause RIP to create a default route entry in the RIP database. The entry will be of type RS (Rip Static). Unless actively filtered out, this default route will be advertised out every interface that is sending RIP. Split horizon does not apply to this route, as it is internally generated. This operates quite similarly to the OSPF **default-information originate always** command.

Example `awplus# configure terminal`
`awplus(config)# router rip`
`awplus(config-router)# default-information originate`

default-metric (RIP)

Overview Use this command to specify the metrics to be assigned to redistributed RIP routes. Use the **no** variant of this command to reset the RIP metric back to its default (1).

Syntax `default-metric <metric>`
`no default-metric [<metric>]`

Parameter	Description
<metric>	<1-16> Specifies the value of the default metric.

Default By default, the RIP metric value is set to 1.

Mode RIP Router Configuration

Usage notes This command is used with the [redistribute \(RIP\)](#) command to make the routing protocol use the specified metric value for all redistributed routes, regardless of the original protocol that the route has been redistributed from.

Examples This example assigns the cost of 10 to the routes that are redistributed into RIP.

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# default-metric 10
awplus(config-router)# redistribute ospf
awplus(config-router)# redistribute connected
```

Related commands [redistribute \(RIP\)](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

distance (RIP)

Overview This command sets the administrative distance for RIP routes. Your device uses this value to select between two or more routes to the same destination obtained from two different routing protocols. The route with the smallest administrative distance value is added to the Forwarding Information Base (FIB). For more information, see the [Route Selection Feature Overview and Configuration Guide](#).

The **no** variant of this command sets the administrative distance for the RIP route to the default of 120.

Syntax `distance <1-255> [<ip-addr/prefix-length>]`
`no distance [<1-255>] [<ip-addr/prefix-length>]`

Parameter	Description
<1-255>	The administrative distance value you are setting for this RIP route.
<ip-addr/prefix-length>	The network IP address and prefix-length that you are changing the administrative distance for.

Mode RIP Router Configuration

Examples To set the administrative distance to 8 for the RIP routes within the 10.0.0.0/8 network, use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# distance 8 10.0.0.0/8
```

To set the administrative distance to the default of 120 for the RIP routes within the 10.0.0.0/8 network, use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no distance 8 10.0.0.0/8
```

Command changes Version 5.4.6-2.1: VRF-lite support added.

distribute-list (RIP)

Overview Use this command to filter incoming or outgoing route updates using the prefix-list.

Use the **no** variant of this command to disable this feature.

Syntax `distribute-list prefix <prefix-list> {in|out} [<interface>]`
`no distribute-list prefix <prefix-list> {in|out} [<interface>]`

Parameter	Description
<code>prefix</code>	Filter prefixes in routing updates.
<code><prefix-list></code>	Specifies the name of the IPv4 prefix-list to use.
<code>in</code>	Filter incoming routing updates.
<code>out</code>	Filter outgoing routing updates.
<code><interface></code>	The interface on which the filtering applies.

Default Disabled

Mode RIP Router Configuration

Usage notes Filter out incoming or outgoing route updates using a prefix-list. If you do not specify the name of the interface, the filter will be applied to all interfaces.

Examples To apply a prefix list called 'myfilter' to filter incoming routing updates on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# distribute-list prefix myfilter in eth1
```

Command changes Version 5.4.6-2.1: VRF-lite support added.

fullupdate (RIP)

Overview Use this command to specify which routes RIP should advertise when performing a triggered update. By default, when a triggered update is sent, RIP will only advertise those routes that have changed since the last update. When **fullupdate** is configured, the device advertises the full RIP route table in outgoing triggered updates, including routes that have not changed. This enables faster convergence times, or allows inter-operation with legacy network equipment, but at the expense of larger update messages.

Use the **no** variant of this command to disable this feature.

Syntax fullupdate
no fullupdate

Default By default this feature is disabled.

Mode RIP Router Configuration

Example To enable the fullupdate (RIP) function, use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# fullupdate
```

Command changes Version 5.4.6-2.1: VRF-lite support added.

ip summary-address rip

Overview Use this command to configure a summary IP address on a RIPv2 interface.

Use the **no** variant of this command to remove a summary IP address from a selected RIPv2 interface.

Syntax `ip summary-address rip {<ip-address/prefix-length>}`
`no ip summary-address rip {<ip-address/prefix-length>}`

Parameter	Description
<code><ip-address/prefix-length></code>	The summary IPv4 address to be advertised

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes Route summarization is a technique that helps network administrators reduce the size of the routing tables by advertising a single super-network that covers a range of subnets.

You statically configure an IP summary address on a router interface. The router then advertises the summary address downstream through this interface. This means that:

- all the routers that are downstream from the configured interface will receive only the summary route, and none of the child routes via the RIP advertisement.
- As long as at least one of the child routes is valid, the router will propagate the summary route. But when the last child that is part of the summarized range disappears, then the router will stop advertising the summary route through the interface.

This command will be rejected if there is no IP address configured on the interface.

NOTE: Manual route summarization is not supported when the interface/router is running in RIPv1.

Example The subnets 10.4.1.0/24, 10.4.2.128/25 and 10.4.3.0/24 can be summarized and advertised as 10.4.0.0/16 on eth1 using the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip summary-address rip 10.4.0.0/16
```

Related commands [show ip rip database](#)
[show ip protocols rip](#)

Command changes Version 5.4.8-0.2 command added

ip prefix-list

Overview Use this command to create an entry for an IPv4 prefix list.

Use the **no** variant of this command to delete the IPv4 prefix-list entry.

Syntax

```
ip prefix-list <list-name> [seq <1-429496725>] {deny|permit}
{any|<ip-prefix>} [ge <0-32>] [le <0-32>]

ip prefix-list <list-name> description <text>

ip prefix-list sequence-number

no ip prefix-list <list-name> [seq <1-429496725>]

no ip prefix-list <list-name> [description <text>]

no ip prefix-list sequence-number
```

Parameter	Description
<list-name>	Specifies the name of a prefix list.
seq <1-429496725>	Sequence number of the prefix list entry.
deny	Specifies that the prefixes are excluded from the list.
permit	Specifies that the prefixes are included in the list.
<ip-prefix>	Specifies the IPv4 address and length of the network mask in dotted decimal in the format A.B.C.D/M.
any	Any prefix match. Same as 0.0.0.0/0 le 32 .
ge<0-32>	Specifies the minimum prefix length to be matched.
le<0-32>	Specifies the maximum prefix length to be matched.
<text>	Text description of the prefix list.
sequence-number	Specify sequence numbers included or excluded in prefix list.

Mode Global Configuration

Usage notes When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the **seq** parameter and place common permits or denials towards the top of the list. If you do not use the **seq** parameter, the sequence values are generated in a sequence of 5.

The parameters **ge** and **le** specify the range of the prefix lengths to be matched. When setting these parameters, set the **le** value to be less than 32, and the **ge** value to be less than or equal to the **le** value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.

Example In the following sample configuration, the last **ip prefix-list** command in the below list matches all, and the first **ip prefix-list** command denies the IP network 76.2.2.0:

```
awplus(config)# router bgp 100
awplus(config-router)# network 172.1.1.0
awplus(config-router)# network 172.1.2.0
awplus(config-router)# neighbor 10.6.5.3 remote-as 300
awplus(config-router)# neighbor 10.6.5.3 prefix-list mylist out
awplus(config-router)# exit
awplus(config)# ip prefix-list mylist seq 5 deny 76.2.2.0/24
awplus(config)# ip prefix-list mylist seq 100 permit any
```

To deny the IP addresses between 10.0.0.0/14 (10.0.0.0 255.252.0.0) and 10.0.0.0/22 (10.0.0.0 255.255.252.0) within the 10.0.0.0/8 (10.0.0.0 255.0.0.0) addressing range, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip prefix-list mylist seq 12345 deny 10.0.0.0/8
ge 14 le 22
```

Related commands

- [neighbor prefix-list](#)
- [clear ip prefix-list](#)
- [show ip prefix-list](#)

ip rip authentication key-chain

Overview Use this command to enable RIPv2 authentication on an interface and specify the name of the key chain to be used.

Use the **no** variant of this command to disable this function.

Syntax `ip rip authentication key-chain <key-chain-name>`
`no ip rip authentication key-chain`

Parameter	Description
<code><key-chain-name></code>	Specify the name of the key chain. This is an alpha-numeric string, but it cannot include spaces.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes Use this command to perform authentication on the interface. Not configuring the key chain results in no authentication at all.

The AlliedWare Plus™ implementation provides the choice of configuring authentication for single key or multiple keys at different times. Use the [ip rip authentication string](#) command for single key authentication. Use the [ip rip authentication key-chain](#) command for multiple keys authentication. See the [RIP Feature Overview and Configuration Guide](#) for illustrated RIP configuration examples.

For multiple key authentication, use the following steps to configure a route to enable RIPv2 authentication using multiple keys at different times:

1) Define a key chain with a key chain name, using the following commands:

```
awplus# configure terminal
awplus(config)# key chain <key-chain-name>
```

2) Define a key on this key chain, using the following command:

```
awplus(config-keychain)# key <keyid>
```

3) Define the password used by the key, using the following command:

```
awplus(config-keychain-key)# key-string <key-password>
```

4) Enable authentication on the desired interface and specify the key chain to be used, using the following commands:

```
awplus# configure terminal
awplus(config)# interface <id>
awplus(config-if)# ip rip authentication key-chain
<key-chain-name>
```

- 5) Specify the mode of authentication for the given interface (text or MD5), using the following command:

```
awplus(config-if)# ip rip authentication mode {md5|text}
```

Example 1 To use the key chain named 'mykey' on the interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip rip authentication key-chain mykey
```

Example 2 In the following example of a configuration for multiple keys authentication, a password 'toyota' is set for key 1 in key chain 'cars'. Authentication is enabled on eth1 and the authentication mode is set to MD5:

```
awplus# configure terminal
awplus(config)# key chain cars
awplus(config-keychain)# key 1
awplus(config-keychain-key)# key-string toyota
awplus(config-keychain-key)# accept-lifetime 10:00:00 Oct 08 2021 duration 43200
awplus(config-keychain-key)# send-lifetime 10:00:00 Oct 08 2021 duration 43200
awplus(config-keychain-key)# exit
awplus(config-keychain)# exit
awplus(config)# interface eth1
awplus(config-if)# ip rip authentication key-chain cars
awplus(config-if)# ip rip authentication mode md5
```

Related commands

[accept-lifetime](#)
[send-lifetime](#)
[ip rip authentication mode](#)
[ip rip authentication string](#)
[key](#)
[key chain](#)

ip rip authentication mode

Overview Use this command to specify the type of authentication mode used for RIP v2 packets.

Use the **no** variant of this command to restore clear text authentication.

Syntax `ip rip authentication mode {md5|text}`
`no ip rip authentication mode`

Parameter	Description
md5	Uses the keyed MD5 authentication algorithm.
text	Specifies clear text or simple password authentication.

Default Text authentication is enabled

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes The AlliedWare Plus™ implementation provides the choice of configuring authentication for single key or multiple keys at different times. Use the [ip rip authentication string](#) command for single key authentication. Use the [ip rip authentication key-chain](#) command for multiple keys authentication. See the [RIP Feature Overview and Configuration Guide](#) for illustrated RIP configuration examples.

Usage: single key Use the following steps to configure a route to enable RIPv2 authentication using a single key or password:

- 1) Define the authentication string or password used by the key for the desired interface, using the following commands:

```
awplus# configure terminal
awplus(config)# interface <id>
awplus(config-if)# ip rip authentication string <auth-string>
```

- 2) Specify the mode of authentication for the given interface (text or MD5), using the following commands:

```
awplus# configure terminal
awplus(config)# interface <id>
awplus(config-if)# ip rip authentication mode {md5|text}
```


Usage: multiple key For multiple keys authentication, use the following steps to configure a route to enable RIPv2 authentication using multiple keys at different times:

- 1) Define a key chain with a key chain name, using the following commands:

```
awplus# configure terminal
awplus(config)# key chain <key-chain-name>
```

- 2) Define a key on this key chain using the following command:

```
awplus(config-keychain)# key <keyid>
```

- 3) Define the password used by the key, using the following command:

```
awplus(config-keychain-key)# key-string <key-password>
```

- 4) Enable authentication on the desired interface and specify the key chain to be used, using the following commands:

```
awplus(config-if)# ip rip authentication key-chain
<key-chain-name>
```

- 5) Specify the mode of authentication for the given interface (text or MD5), using the following commands:

```
awplus(config-if)# ip rip authentication mode {md5|text}
```

Example 1 To use MD5 authentication on the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip rip authentication mode md5
```

Example 2 In the following example of a configuration for multiple keys authentication, a password 'toyota' is set for key 1 in key chain 'cars'. Authentication is enabled on eth1 and the authentication mode is set to MD5:

```
awplus# configure terminal
awplus(config)# key chain cars
awplus(config-keychain)# key 1
awplus(config-keychain-key)# key-string toyota
awplus(config-keychain-key)# accept-lifetime 10:00:00 Oct 08
2016 duration 43200
awplus(config-keychain-key)# send-lifetime 10:00:00 Oct 08 2016
duration 43200
awplus(config-keychain-key)# exit
awplus(config-keychain)# exit
awplus(config)# interface eth1
awplus(config-if)# ip rip authentication key-chain cars
awplus(config-if)# ip rip authentication mode md5
```

Related commands [ip rip authentication string](#)
[ip rip authentication key-chain](#)

ip rip authentication string

Overview Use this command to specify the authentication string or password used by a key. Use the **no** variant of this command to remove the authentication string.

Syntax `ip rip authentication string <auth-string>`
`no ip rip authentication string`

Parameter	Description
<code><auth-string></code>	The authentication string or password used by a key. It is an alphanumeric string and can include spaces.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes The AlliedWare Plus™ implementation provides the choice of configuring authentication for single key or multiple keys at different times. Use this command to specify the password for a single key on an interface. Use the [ip rip authentication key-chain](#) command for multiple keys authentication. For information about configuring RIP, see the [RIP Feature Overview and Configuration Guide](#).

Use the following steps to configure a route to enable RIPv2 authentication using a single key or password:

- 1) Define the authentication string or password used by the key for the desired interface, using the following commands:

```
awplus# configure terminal
awplus(config)# interface <id>
```

- 2) Specify the mode of authentication for the given interface (text or MD5), using the following commands:

```
awplus# configure terminal
awplus(config-if)# ip rip authentication string <auth-string>
awplus(config)# interface <id>
awplus(config-if)# ip rip authentication mode {md5|text}
```

Example To specify 'mykey' as the authentication string and use MD5 authentication for the interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip rip authentication string mykey
awplus(config-if)# ip rip authentication mode md5
```

Any RIP packet received on that interface should have the same string as its password.

Related commands [ip rip authentication key-chain](#)
[ip rip authentication mode](#)

ip rip receive-packet

Overview Use this command to configure the interface to enable the reception of RIP packets.

Use the **no** variant of this command to disable this feature.

Syntax `ip rip receive-packet`
`no ip rip receive-packet`

Default Enabled

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Example To turn on packet receiving on the interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip rip receive-packet
```

Related commands [ip rip send-packet](#)

ip rip receive version

Overview Use this command to specify the version of RIP packets accepted on an interface and override the setting of the version command.

Use the **no** variant of this command to use the setting specified by the [version \(RIP\)](#) command.

Syntax `ip rip receive version [1] [2]`
`no ip rip receive version`

Parameter	Description
1	Specifies acceptance of RIP version 1 packets on the interface.
2	Specifies acceptance of RIP version 2 packets on the interface.

Default Version 2

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command applies to a specific interface and overrides the version specified by the [version \(RIP\)](#) command.

RIP can be run in version 1 or version 2 mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces.

Example To set the interface eth1 to receive both RIP version 1 and 2 packets, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip rip receive version 1 2
```

Related commands [version \(RIP\)](#)

ip rip send-packet

Overview Use this command to enable sending RIP packets through the current interface.
Use the **no** variant of this command to disable this feature.

Syntax `ip rip send-packet`
`no ip rip send-packet`

Default Enabled

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Example To turn on packet sending on the interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip rip send-packet
```

Related commands [ip rip receive-packet](#)

ip rip send version

Overview Use this command in Interface Configuration mode to specify the version of RIP packets sent on an interface and override the setting of the [version \(RIP\)](#) command. This mechanism causes RIP version 2 interfaces to send multicast packets instead of broadcasting packets.

Use the **no** variant of this command to use the setting specified by the [version \(RIP\)](#) command.

Syntax `ip rip send version {1|2|1 2|2 1}`
`no ip rip send version`

Parameter	Description
1	Specifies the sending of RIP version 1 packets out of an interface.
2	Specifies the sending of RIP version 2 packets out of an interface.
1 2	Specifies the sending of both RIP version 1 and RIP version 2 packets out of an interface.
2 1	Specifies the sending of both RIP version 2 and RIP version 1 packets out of an interface.

Default Version 2

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command applies to a specific interface and overrides the version specified by the [version \(RIP\)](#) command.

RIP can be run in version 1 or version 2 mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces. Selecting version parameters 1 2 or 2 1 sends RIP version 1 and 2 packets.

Use the [ip rip send version 1-compatible](#) command in an environment where you cannot send multicast packets. For example, in environments where multicast is not enabled and where hosts do not listen to multicast.

Examples To set the interface eth1 to send both RIP version 1 and 2 packets, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip rip send version 1 2
```

To set the interface eth1 to use the RIP version specified by the [version \(RIP\)](#) command, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip rip send version
```

Related commands [ip rip send version 1-compatible](#)
[version \(RIP\)](#)

ip rip send version 1-compatible

Overview Use this command in Interface Configuration mode to send RIP version 1 compatible packets from a RIP version 2 interface to other RIP Interfaces. This mechanism causes RIP version 2 interfaces to send broadcast packets instead of multicasting packets, and is used in environments where multicast is not enabled or where hosts do not listen to multicast.

Use the **no** variant of this command to use the setting specified by the [version \(RIP\)](#) command, and disable the broadcast of RIP version 2 packets that are sent as broadcast packets.

Syntax `ip rip send version 1-compatible`
`no ip rip send version`

Parameter	Description
1-compatible	Specify this parameter to send RIP version 1 compatible packets from a version 2 RIP interface to other RIP interfaces. This mechanism causes version 2 RIP interfaces to broadcast packets instead of multicasting packets.

Default RIP version 2 is enabled by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command applies to a specific interface and overrides the version specified by the [version \(RIP\)](#) command.

RIP can be run in version 1 compatible mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces.

Use the [ip rip send version](#) command in an environment where you can send multicast packets, for example, in environments where multicast is enabled and where hosts listen to multicast.

Example To set the interface eth1 to send RIP version 1- compatible packets, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip rip send version 1-compatible
```

Related commands [ip rip send version](#)
[version \(RIP\)](#)

ip rip split-horizon

Overview Use this command to turn on the split-horizon mechanism on the interface.
Use the **no** variant of this command to disable this mechanism.

Syntax `ip rip split-horizon [poisoned]`
`no ip rip split-horizon`

Parameter	Description
poisoned	Performs split-horizon with poison-reverse. See "Usage" below for more information.

Default Split horizon poisoned

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes Use this command to avoid including routes in updates sent to the same gateway from which they were learned. Without the **poisoned** parameter, using this command causes routes learned from a neighbor to be omitted from updates sent to that neighbor. With the **poisoned** parameter, using this command causes such routes to be included in updates, but sets their metrics to infinity. This advertises that these routes are not reachable.

Example To turn on split horizon poisoned on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip rip split-horizon poisoned
```

key

Overview Use this command to manage, add and delete authentication keys in a key-chain.
Use the **no** variant of this command to delete the authentication key.

Syntax `key <keyid>`
`no key <keyid>`

Parameter	Description
<keyid>	<0-2147483647> Key identifier number.

Mode Keychain Configuration

Usage This command allows you to enter the keychain-key mode where a password can be set for the key.

Example The following example configures a key number 1 and shows the change into a **keychain- key** command mode prompt.

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)#
```

Related commands [key chain](#)
[key-string](#)
[accept-lifetime](#)
[send-lifetime](#)

key chain

Overview Use this command to enter the key chain management mode and to configure a key chain with a key chain name.

Use the **no** variant of this command to remove the key chain and all configured keys.

Syntax `key chain <key-chain-name>`
`no key chain <key-chain-name>`

Parameter	Description
<code><key-chain-name></code>	Specify the name of the key chain to manage.

Mode Global Configuration

Usage This command allows you to enter the keychain mode from which you can specify keys on this key chain.

Example The following example shows the creation of a key chain named `mychain` and the change into **keychain** mode prompt.

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)#
```

Related commands [key](#)
[key-string](#)
[accept-lifetime](#)
[send-lifetime](#)

key-string

Overview Use this command to define the password to be used by a key.
Use the **no** variant of this command to remove a password.

Syntax `key-string <key-password>`
`no key-string`

Parameter	Description
<code><key-password></code>	A string of characters to be used as a password by the key.

Mode Keychain-key Configuration

Usage Use this command to specify passwords for different keys.

Examples In the following example, the password for `key1` in the key chain named `mychain` is set to password **prime**:

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# key-string prime
```

In the following example, the password for `key1` in the key chain named `mychain` is removed:

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# no key-string
```

Related commands

- [key](#)
- [key chain](#)
- [accept-lifetime](#)
- [send-lifetime](#)

maximum-prefix

Overview Use this command to configure the maximum number of RIP routes stored by the device.

Use the **no** variant of this command to disable all limiting of the number of RIP routes stored by the device.

Syntax `maximum-prefix <maxprefix> [<threshold>]`
`no maximum-prefix`

Parameter	Description
<code><maxprefix></code>	<code><1-65535></code> The maximum number of RIP routes allowed.
<code><threshold></code>	<code><1-100></code> Percentage of maximum routes to generate a warning. The default threshold is 75%.

Mode Router Configuration

Example To configure the maximum number of RIP routes to 150, use the following command:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# maximum-prefix 150
```

neighbor (RIP)

Overview Use this command to specify a neighbor router. It is used for each router to which you wish to send unicast RIP updates.

Use the **no** variant of this command to stop sending unicast updates to the specific router.

Syntax `neighbor <ip-address>`
`no neighbor <ip-address>`

Parameter	Description
<code><ip-address></code>	The IP address of a neighboring router with which the routing information will be exchanged.

Default Disabled

Mode Router Configuration

Usage Use this command to exchange nonbroadcast routing information. It can be used multiple times for additional neighbors.

The [passive-interface \(RIP\)](#) command disables sending routing updates on an interface. If you want to send routing updates only to specific neighbors, use the [passive-interface \(RIP\)](#) command and this **neighbor** command together.

Example To specify the neighbor router to 1.1.1.1, use the following command:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# passive-interface eth1
awplus(config-router)# neighbor 1.1.1.1
```

Related commands [passive-interface \(RIP\)](#)

network (RIP)

Overview Use this command to activate the transmission of RIP routing information on the defined network.

Use the **no** variant of this command to remove the specified network or interface as one that runs RIP.

Syntax `network {<network-address>[/<subnet-mask>]|<interface>}`
`no network {<network-address>[/<subnet-mask>]|<interface>}`

Parameter	Description
<code><network-address>[/<subnet-mask>]</code>	Specifies the network address to run RIP. Entering a subnet mask (or prefix length) for the network address is optional. Where no mask is entered, the device will attempt to apply a mask that is appropriate to the class (A, B, or C) of the address entered, e.g. an IP address of 10.0.0.0 will have a prefix length of 8 applied to it.
<code><interface></code>	Specify an interface to run RIP.

Default Disabled

Mode RIP Router Configuration

Usage notes Use this command to specify networks, by IP address or interface, to which routing updates will be sent and received. The connected routes corresponding to the specified network will be automatically advertised in RIP updates. RIP updates will be sent and received within the specified network.

Example Use the following commands to activate RIP routing updates on network 172.16.20.0/24:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# network 172.16.20.0/24
```

Related commands [show ip rip](#)
[show running-config](#)
[clear ip rip route](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

passive-interface (RIP)

Overview Use this command to block RIP broadcasts on the interface.
Use the **no** variant of this command to disable this function.

Syntax `passive-interface <interface>`
`no passive-interface <interface>`

Parameter	Description
<code><interface></code>	Specifies the interface name.

Default Disabled

Mode RIP Router Configuration

Example Use the following commands to block RIP broadcasts on eth1:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# passive-interface eth1
```

Related commands [show ip rip](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

recv-buffer-size (RIP)

Overview Use this command to run-time configure the RIP UDP (User Datagram Protocol) receive-buffer size to improve UDP reliability by avoiding UDP receive buffer overrun.

Use the **no** variant of this command to reset the configured RIP UDP receive-buffer size to the system default (196608 bits).

Syntax `recv-buffer-size <8192-2147483647>`
`no recv-buffer-size [<8192-2147483647>]`

Parameter	Description
<code><8192-2147483647></code>	Specify the RIP UDP (User Datagram Protocol) buffer size value in bits.

Default 196608 bits is the system default when reset using the **no** variant of this command.

Mode Router Configuration

Examples To run-time configure the RIP UDP, use the following commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# recv-buffer-size 23456789
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no recv-buffer-size 23456789
```

redistribute (RIP)

Overview Use this command to redistribute information from other routing protocols into RIP.

Use the **no** variant of this command to disable the specified redistribution. The parameters **metric** and **route-map** may be used with the **no** variant, but have no effect.

Syntax `redistribute {connected|static|ospf|bgp} [metric <0-16>]
[route-map <route-map>]
no redistribute {connected|static|ospf|bgp} [metric] [route-map]`

Parameter	Description
route-map	Optional. Specifies route-map that controls how routes are redistributed.
<route-map>	Optional. The name of the route map.
connected	Redistribute from connected routes.
static	Redistribute from static routes.
ospf	Redistribute from Open Shortest Path First (OSPF).
bgp	Redistribute from Border Gateway Protocol (BGP).
metric <0-16>	Optional. Sets the value of the metric that will be applied to routes redistributed into RIP from other protocols. If a value is not specified, and no value is specified using the default-metric (RIP) command, the default is one.

Default By default, the RIP metric value is set to 1.

Mode RIP Router Configuration

Example To apply the metric value 15 to static routes being redistributed into RIP, use the commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# redistribute static metric 15
```

Related commands [default-metric \(RIP\)](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

restart rip graceful

Overview Use this command to force the RIP process to restart, and optionally set the grace-period.

Syntax `restart rip graceful [grace-period <1-65535>]`

Mode Privileged Exec

Default The default RIP grace-period is 60 seconds.

Usage notes After this command is executed, the RIP process immediately shuts down. It notifies the system that RIP has performed a graceful shutdown. Routes that have been installed into the route table by RIP are preserved until the specified grace-period expires.

When a **restart rip graceful** command is issued, the RIP configuration is reloaded from the last saved configuration. Ensure you first enter the command [copy running-config startup-config](#).

Example To apply a restart rip graceful setting, grace-period to 100 seconds use the following commands:

```
awplus# copy running-config startup-config
awplus# restart rip graceful grace-period 100
```

rip restart grace-period

Overview Use this command to change the grace period of RIP graceful restart.
Use the **no** variant of this command to disable this function.

Syntax `rip restart grace-period <1-65535>`
`no rip restart grace-period <1-65535>`

Mode Global Configuration

Default The default RIP grace-period is 60 seconds.

Usage notes Use this command to enable the **Graceful Restart** feature on the RIP process.
Entering this command configures a grace period for RIP.

Example `awplus# configure terminal`
`awplus(config)# rip restart grace-period 200`

route (RIP)

Overview Use this command to add a static RIP route.
Use the **no** variant of this command to remove a static RIP route.

Syntax `route <ip-addr/prefix-length>`
`no route <ip-addr/prefix-length>`

Parameter	Description
<code><ip-addr/prefix-length></code>	The IPv4 address and prefix length.

Default No static RIP route is added by default.

Mode RIP Router Configuration

Usage notes Use this command to add a static RIP route. After adding the RIP route, the route can be checked in the RIP routing table.

Example To create a static RIP route to IP subnet 192.168.1.0/24, use the following commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# route 192.168.1.0/24
```

Related commands [show ip rip](#)
[clear ip rip route](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

router rip

Overview Use this global command to enter Router Configuration mode to enable the RIP routing process.

Use the **no** variant of this command to disable the RIP routing process.

Syntax `router rip`
`no router rip`

Mode Global Configuration

Example This command is used to begin the RIP routing process:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# version 1
awplus(config-router)# network 10.10.10.0/24
awplus(config-router)# network 10.10.11.0/24
awplus(config-router)# neighbor 10.10.10.10
```

Related commands [network \(RIP\)](#)
[version \(RIP\)](#)

send-lifetime

Overview Use this command to specify the time period during which the authentication key on a key chain can be sent.

Syntax `send-lifetime <start-date> {<end-date>|
duration <seconds>|infinite}`
`no send-lifetime`

Parameter	Description
<start-date>	Specifies the start time and date in the format: <hh:mm:ss> <day> <month> <year> or <hh:mm:ss> <month> <day> <year>, where:
	<hh:mm:ss> The time of the day, in hours, minutes and seconds
	<day> <1-31> The day of the month
	<month> The month of the year (the first three letters of the month, for example, Jan)
	<year> <1993-2035> The year
<end-date>	Specifies the end time and date in the format: <hh:mm:ss> <day> <month> <year> or <hh:mm:ss> <month> <day> <year>, where:
	<hh:mm:ss> The time of the day, in hours, minutes and seconds
	<day> <1-31> The day of the month
	<month> The month of the year (the first three letters of the month, for example, Jan)
	<year> <1993-2035> The year
<seconds>	<1-2147483646> Duration of the key in seconds.
infinite	Never expires.

Mode Keychain-key Configuration

Example The following example shows the setting of send-lifetime for key 1 on the key chain named "mychain".

```
awplus# configure terminal
awplus(config)# key chain mychain
awplus(config-keychain)# key 1
awplus(config-keychain-key)# send-lifetime 03:03:01 Jan 3 2016
04:04:02 Dec 6 2016
```


**Related
commands**

- [key](#)
- [key-string](#)
- [key chain](#)
- [accept-lifetime](#)

show debugging rip

Overview Use this command to display the RIP debugging status for these debugging options: nsm debugging, RIP event debugging, RIP packet debugging and RIP nsm debugging.

For information on filtering and saving command output, see the [“Getting_Started with AlliedWare Plus” Feature Overview and Configuration_Guide](#).

Syntax `show debugging rip`

Mode User Exec and Privileged Exec

Usage notes Use this command to display the debug status of RIP.

Example `awplus# show debugging rip`

show ip prefix-list

Overview Use this command to display the IPv4 prefix-list entries.
Note that this command is valid for RIP and BGP routing protocols only.

Syntax `show ip prefix-list [<name>|detail|summary]`

Parameter	Description
<name>	Specify the name of a prefix list in this placeholder.
detail	Specify this parameter to show detailed output for all IPv4 prefix lists.
summary	Specify this parameter to show summary output for all IPv4 prefix lists.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip prefix-list
awplus# show ip prefix-list 10.10.0.98/8
awplus# show ip prefix-list detail
```

Related commands [ip prefix-list](#)

show ip protocols rip

- Overview** Use this command to display RIP process parameters and statistics.
For information on filtering and saving command output, see the [“Getting_Started with AlliedWare Plus” Feature Overview and Configuration_Guide](#).
- Syntax** `show ip protocols rip`
- Mode** User Exec and Privileged Exec
- Example** `awplus# show ip protocols rip`
- Output** Figure 20-1: Example output from the **show ip protocols rip** command

```
Routing Protocol is "rip"
Sending updates every 30 seconds with +/-50%, next due in 12
seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing: connected static
Default version control: send version 2, receive version 2
Interface          Send  Recv   Key-chain
   vlan25           2     2
Routing for Networks:
  10.10.0.0/24
Routing Information Sources:
  Gateway           BadPackets BadRoutes  Distance Last Update
Distance: (default is 120
```

show ip rip

Overview Use this command to show RIP routes.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip rip`

Mode User Exec and Privileged Exec

Example `awplus# show ip rip`

Output Figure 20-2: Example output from the **show ip rip** command

```
awplus#show ip rip
Codes: R - RIP, Rc - RIP connected, Rs - RIP static
       C - Connected, S - Static, O - OSPF, B - BGP
Network      Next Hop Metric From If      Time
C 10.0.1.0/24          1     eth1
S 10.10.10.0/24        1     eth1
C 10.10.11.0/24        1     eth1
S 192.168.101.0/24     1     eth1
R 192.192.192.0/24     1     --
```

Related commands [route \(RIP\)](#)
[network \(RIP\)](#)
[clear ip rip route](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

show ip rip database

Overview Use this command to display information about the RIP database.

For information on filtering and saving command output, see the [“Getting_Started with AlliedWare Plus” Feature Overview and Configuration_Guide](#).

Syntax `show ip rip database [full]`

Parameter	Description
full	Specify the full RIP database including sub-optimal RIP routes.

Mode User Exec and Privileged Exec

Example `awplus# show ip rip database`
`awplus# show ip rip database full`

Related commands [show ip rip](#)

show ip rip interface

Overview Use this command to display information about the RIP interfaces. You can specify an interface name to display information about a specific interface.

Syntax `show ip rip interface [<interface>]`

Parameter	Description
<interface>	The interface to display information about.

Mode User Exec and Privileged Exec

Example `awplus# show ip rip interface`

timers (RIP)

Overview Use this command to adjust routing network timers.

Use the **no** variant of this command to restore the defaults.

Syntax `timers basic <update> <timeout> <garbage>`
`no timers basic`

Parameter	Description
<code><update></code>	<code><5-2147483647></code> Specifies the period at which RIP route update packets are transmitted. The default is 30 seconds.
<code><timeout></code>	<code><5-2147483647></code> Specifies the routing information timeout timer in seconds. The default is 180 seconds. After this interval has elapsed and no updates for a route are received, the route is declared invalid.
<code><garbage></code>	<code><5-2147483647></code> Specifies the routing garbage collection timer in seconds. The default is 120 seconds.

Default Enabled

Mode RIP Router Configuration

Usage notes This command adjusts the RIP timing parameters.

The update timer is the time between sending out updates, that contain the complete routing table, to every neighboring router.

If an update for a given route has not been seen for the time specified by the timeout parameter, that route is no longer valid. However, it is retained in the routing table for a short time, with metric 16, so that neighbors are notified that the route has been dropped.

When the time specified by the garbage parameter expires the metric 16 route is finally removed from the routing table. Until the garbage time expires, the route is included in all updates sent by the router.

All the routers in the network must have the same timers to ensure the smooth operation of RIP throughout the network.

Examples To set the update timer to 30, the routing information timeout timer to 180, and the routing garbage collection timer to 120, use the following command:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# timers basic 30 180 120
```


Command changes Version 5.4.6-2.1: VRF-lite support added.

undebg rip

Overview Use this command to disable the options set for debugging information of RIP events, packets and communication between RIP and NSM.

This command has the same effect as the **no debug rip** command.

Syntax `undebg rip {all|events|nsm|<packet>}`

Parameter	Description
all	Disables all RIP debugging.
events	Disables the logging of RIP events.
nsm	Disables the logging of RIP and NSM communication.
<packet>	packet [recv send] [detail] Disables the debugging of RIP packets.
recv	Disables the logging of received packet information.
send	Disables the logging of sent packet information.
detail	Disables the logging of sent or received RIP packets.

Mode Privileged Exec

Example To disable the options set for debugging RIP information events, use the following command:

```
awplus# undebg rip packet
```

Related commands [debug rip](#)

version (RIP)

Overview Use this command to specify a RIP version used globally by the router.
Use the **no** variant of this command to restore the default version.

Syntax `version {1|2}`
`no version`

Parameter	Description
1 2	Specifies the version of RIP processing.

Default Version 2

Mode RIP Router Configuration

Usage notes RIP can be run in version 1 or version 2 mode. Version 2 has more features than version 1; in particular RIP version 2 supports authentication and classless routing. Once the RIP version is set, RIP packets of that version will be received and sent on all the RIP-enabled interfaces.

Setting the version command has no impact on receiving updates, only on sending them. The [ip rip send version](#) command overrides the value set by the [version \(RIP\)](#) command on an interface-specific basis. The [ip rip receive version](#) command allows you to configure a specific interface to accept only packets of the specified RIP version. The [ip rip receive version](#) command and the [ip rip send version](#) command override the value set by this command.

Examples To specify a RIP version, use the following commands:

```
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# version 1
```

Related commands [ip rip receive version](#)
[ip rip send version](#)
[show running-config](#)

Command changes Version 5.4.6-2.1: VRF-lite support added.

21

RIPng for IPv6 Commands

Introduction

Overview This chapter contains RIPng commands. RIPng (Routing Information Protocol next generation) is an extension of RIPv2 to support IPv6. RFC 2080 specifies RIPng. The differences between RIPv2 and RIPng are:

- RIPng does not support RIP updates authentication
- RIPng does not allow the attachment of arbitrary tags to routes
- RIPng requires the encoding of the next-hop for a set of routes

For more information, see the [RIPng Feature Overview and Configuration Guide](#).

- Command List**
- [“aggregate-address \(IPv6 RIPng\)”](#) on page 698
 - [“clear ipv6 rip route”](#) on page 699
 - [“debug ipv6 rip”](#) on page 700
 - [“default-information originate \(IPv6 RIPng\)”](#) on page 701
 - [“default-metric \(IPv6 RIPng\)”](#) on page 702
 - [“distribute-list \(IPv6 RIPng\)”](#) on page 703
 - [“ipv6 prefix-list”](#) on page 704
 - [“ipv6 rip metric-offset”](#) on page 706
 - [“ipv6 rip split-horizon”](#) on page 708
 - [“ipv6 router rip”](#) on page 709
 - [“neighbor \(IPv6 RIPng\)”](#) on page 710
 - [“passive-interface \(IPv6 RIPng\)”](#) on page 711
 - [“recv-buffer-size \(IPv6 RIPng\)”](#) on page 712
 - [“redistribute \(IPv6 RIPng\)”](#) on page 713
 - [“route \(IPv6 RIPng\)”](#) on page 714

- [“router ipv6 rip”](#) on page 715
- [“show debugging ipv6 rip”](#) on page 716
- [“show ipv6 prefix-list”](#) on page 717
- [“show ipv6 protocols rip”](#) on page 718
- [“show ipv6 rip”](#) on page 719
- [“show ipv6 rip database”](#) on page 720
- [“show ipv6 rip interface”](#) on page 721
- [“timers \(IPv6 RIPng\)”](#) on page 722
- [“undebg ipv6 rip”](#) on page 723

aggregate-address (IPv6 RIPng)

Overview Use this command to add an aggregate route to RIPng.
Use the **no** variant of this command to remove the aggregate route from RIPng.

Syntax `aggregate-address <ipv6-addr/prefix-length>`
`no aggregate-address <ipv6-addr/prefix-length>`

Parameter	Description
<code><ipv6-addr/prefix-length></code>	Specify the IPv6 Address in the format <code>X:X::X:X/Prefix-Length</code> . The prefix-length is a decimal integer between 1 and 128.

Mode Router Configuration

Usage notes The route will not be added to the RIPng database unless the database contains at least one route which is contained within the address range covered by the aggregate route. As soon as there are any such component routes in the RIPng database, then the following occurs:

- the aggregate route is added to the RIPng database
- all the component routes that are within the address range covered by the aggregate route are retained in the RIPng database, but are marked as suppressed routes. The aggregate route will be advertised in RIPng updates, and the component route will no longer be advertised.

Note that simply having a component route in the IPv6 route database is not a sufficient condition for the aggregate route to be included into the RIPng database. The component route(s) must be in the RIPng database before the aggregate route will be included in the RIPng database. There is no restriction on the method by which the component routes have arrived into the RIPng database, it can be by being connected RIP interfaces, by redistribution or by direct inclusion using the **route** command in router IPv6 RIP configuration mode.

Example `awplus# configure terminal`
`awplus(config)# router ipv6 rip`
`awplus(config-router)# aggregate-address 2001:db8::/32`

clear ipv6 rip route

Overview Use this command to clear specific data from the RIPng routing table.

Syntax `clear ipv6 rip route`
`{<ipv6-addr/prefix-length>|all|connected|rip|static|ospf}`

Parameter	Description
<code><ipv6-addr/prefix-length></code>	Specify the IPv6 Address in format <i>X:X::X:X/Prefix-Length</i> . The prefix-length is a decimal integer between 1 and 128. Removes entries which exactly match this destination address from the RIPng routing table.
<code>connected</code>	Removes redistributed connected entries from RIPng routing table.
<code>static</code>	Removes redistributed static entries from the RIPng routing table.
<code>rip</code>	Removes RIPng routes from the RIPng routing table.
<code>ospf</code>	Removes redistributed OSPFv3 routes from the RIPng routing table.
<code>all</code>	Clears the entire RIPng routing table.

Mode Privileged Exec

Example `awplus# clear ipv6 rip route all`
`awplus# clear ipv6 rip route 2001:db8::/32`

debug ipv6 rip

Overview Use this command to enable RIPng debugging and specify debugging for RIPng events, RIPng packets, or RIPng communication with NSM processes.

Use the **no** variant of this command to disable RIPng debugging.

Syntax

```
debug ipv6 rip [all|events|nsm|packet [detail]|recv  
[detail]|send [detail]]  
  
no debug ipv6 rip [all|events|nsm|packet [detail]|recv  
[detail]|send [detail]]
```

Parameter	Description
all	Displays all RIPng debugging showing RIPng events debug information, RIPng received packets information, and RIPng sent packets information.
events	Displays RIPng events debug information.
nsm	Displays RIPng and NSM communication.
packet	Displays RIPng packets only.
recv	Displays information for received packets.
send	Displays information for sent packets.
detail	Displays detailed information for the sent or received packet.

Default RIPng debugging is disabled by default.

Mode Privileged Exec and Global Configuration

Example

```
awplus# debug ipv6 rip events  
awplus# debug ipv6 rip packet send detail  
awplus# debug ipv6 rip nsm
```

Related commands [undebug ipv6 rip](#)

default-information originate (IPv6 RIPng)

Overview Use this command to generate a default route into RIPng.
Use the **no** variant of this command to disable this feature.

Syntax default-information originate
no default-information originate

Default Disabled

Mode Router Configuration

Example awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# default-information originate

default-metric (IPv6 RIPng)

Overview Use this command to specify the metrics to be assigned to redistributed RIPng routes.

Use the **no** variant of this command to reset the RIPng metric back to its default (1).

Syntax `default-metric <1-16>`
`no default-metric [<1-16>]`

Parameter	Description
<1-16>	Metric value.

Default By default, the RIPng metric value is set to 1.

Mode Router Configuration

Usage This command is used with the [redistribute \(IPv6 RIPng\)](#) command to make the routing protocol use the specified metric value for all redistributed RIPng routes, regardless of the original protocol that the route has been redistributed from.

Note, this metric is not applied to routes that are brought into RIPng by using the **route** command in router IPv6 RIP configuration mode. This metric is, though, applied to any RIPng aggregate routes that have been brought into the RIPng database due to the presence of a component route that was redistributed into RIPng.

Also note that the default-metric is applied to routes redistributed into RIPng with no metric assignment in the routemap associated with redistribution.

Example

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# default-metric 8
```

Related commands [ipv6 rip metric-offset](#)
[redistribute \(IPv6 RIPng\)](#)

distribute-list (IPv6 RIPng)

Overview Use this command to filter incoming or outgoing route updates using the prefix-list.

Use the **no** variant of this command to disable this feature.

Syntax `distribute-list [prefix <prefix-list-name>] [in|out]
[<interface>]`
`no distribute-list [prefix <prefix-list-name>] [in|out]
[<interface>]`

Parameter	Description
<prefix-list-name>	Filter prefixes in routing updates. Specify the name of the IPv6 prefix-list to use.
<interface>	The interface for which distribute-list applies.
in	Filter incoming routing updates.
out	Filter outgoing routing updates.

Default Disabled

Mode Router Configuration

Usage notes Filter out incoming or outgoing route updates using the prefix-list. If you do not specify the name of the interface, the filter is applied to all the interfaces.

Example To filter incoming or outgoing route updates, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# distribute-list prefix myfilter in eth1
```

Related commands [ipv6 nd prefix](#)

ipv6 prefix-list

Overview Use this command to create an IPv6 prefix list or an entry in an existing prefix list.

Use the **no** variant of this command to delete a whole prefix list, a prefix list entry, or a description.

Syntax

```
ipv6 prefix-list <list-name> [seq <1-429496725>] {deny|permit}
{any|<ipv6-prefix>} [ge <0-128>] [le <0-128>]

ipv6 prefix-list <list-name> description <text>

no ipv6 prefix-list <list-name> [seq <1-429496725>]

no ipv6 prefix-list <list-name> [description <text>]
```

Parameter	Description
<list-name>	Specifies the name of a prefix list.
seq <1-429496725>	Sequence number of the prefix list entry.
deny	Specifies that the prefixes are excluded from the list.
permit	Specifies that the prefixes are included in the list.
<ipv6-prefix>	Specifies the IPv6 prefix and prefix length in hexadecimal in the format X:X::X:X/M.
any	Any prefix match. Same as ::0/0 le 128.
ge <0-128>	Specifies the minimum prefix length to be matched.
le <0-128>	Specifies the maximum prefix length to be matched.
description	Prefix list specific description.
<text>	Up to 80 characters of text description of the prefix list.

Mode Global Configuration

Usage notes When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the **seq** parameter and place common permits or denials towards the top of the list. If you do not use the **seq** parameter, the sequence values are generated in a sequence of 5.

The parameters **ge** and **le** specify the range of the prefix lengths to be matched. The parameters **ge** and **le** are only used if an ip-prefix is stated. When setting these parameters, set the **le** value to be less than 128, and the **ge** value to be less than or equal to the **le** value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.

Example To check the first 32 bits of the prefix 2001:db8:: and that the subnet mask must be greater than or equal to 34 and less than or equal to 40, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 prefix-list mylist seq 12345 permit
2001:db8::/32 ge 34 le 40
```

Related commands

- match ipv6 address
- show ipv6 prefix-list
- show running-config ipv6 prefix-list

ipv6 rip metric-offset

Overview Use this command to increment the metric value on incoming routes for a specified interface. This command can be used to artificially inflate the metric value for routes learned on the specified interface. Routes learned on the specified interface are only used if the routes to the same destination with a lower metric value in the routing table are down.

Use the **no** variant of this command to reset the metric value on incoming routes to the default value (1). You can set the metric value for redistributed routes with [default-metric \(IPv6 RIPng\)](#) and [redistribute \(IPv6 RIPng\)](#) commands in Router Configuration mode.

Syntax `ipv6 rip metric-offset <1-16>`
`no ipv6 rip metric-offset <1-16>`

Parameter	Description
<1-16>	Specify an increment to the metric value on an incoming route. The metric value for RIPng routes is the hop count for the route.

Default The default RIPng metric value is 1.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes When a RIPng route is received on an interface, the metric value for the interface set by this command is added to the metric value of the route in the routing table. Note this command only increments the metric for incoming routes on a specified interface. Increasing the metric value for an interface increases the metric value of routes received on that interface. This changes the route selected from the routing table.

The RIPng metric is the hop count. At regular intervals of the routing update timer (which has a default value of 30 seconds), and at the time of change in the topology, the RIPng router sends update messages to other routers. The listening routers update their route table with the new route, and increase the metric value of the path by one (referred to as a hop count). The router recognizes the IPv6 address advertising router as the next hop, then sends the routing updates to other routers. A maximum allowable hop count is 15. If a router reaches a metric value of 16 or more, the destination is identified as unreachable.

For information about how AlliedWare Plus adds routes, see the [“Route Selection” Feature Overview and Configuration Guide](#). See also the [default-metric \(IPv6 RIPng\)](#) and [redistribute \(IPv6 RIPng\)](#) commands to specify the metric for redistributed RIPng routes.

Examples To increment the metric-offset on the PPP interface ppp0, enter the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# exit
awplus(config)# interface ppp0
awplus(config-if)# ipv6 rip metric-offset
```

To reset the metric-offset on the PPP interface ppp0 to the default value, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 router rip
```

Related commands [default-metric \(IPv6 RIPng\)](#)
[show running-config](#)

ipv6 rip split-horizon

Overview Use this command to perform the split-horizon action on the interface. The default is split-horizon with poisoned reverse.

Use the **no** variant of this command to disable this function.

Syntax `ipv6 rip split-horizon [poisoned]`
`no ipv6 rip split-horizon`

Parameter	Description
<code>split-horizon</code>	Perform split-horizon without poisoned reverse
<code>poisoned</code>	Performs split-horizon with poisoned reverse.

Default Split-horizon with poisoned reverse is the default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes Use this command to avoid including routes in updates sent to the same gateway from which they were learned. Using the **split horizon** command omits routes learned from one neighbor, in updates sent to that neighbor. Using the **poisoned** parameter with this command includes such routes in updates, but sets their metrics to infinity. Thus, advertising that these routes are not reachable.

Examples To perform split-horizon with poisoned reverse on the PPP interface ppp0, enter the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# exit
awplus(config)# interface ppp0
awplus(config-if)# ipv6 rip split-horizon poisoned
```

To disable split-horizon on the PPP interface ppp0, enter the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 rip split-horizon
```

Related Commands [show running-config](#)

ipv6 router rip

- Overview** Use this command to enable RIPng routing on an interface.
Use the **no** variant of this command to disable RIPng routing on an interface.
- Syntax** `ipv6 router rip`
`no ipv6 router rip`
- Default** RIPng routing is disabled by default.
- Mode** Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.
- Examples** To enable RIPng routing on the PPP interface ppp0, enter the commands:
- ```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# exit
awplus(config)# interface ppp0
awplus(config-if)# ipv6 router rip
```
- To disable RIPng routing on the PPP interface ppp0, enter the commands:
- ```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 router rip
```

neighbor (IPv6 RIPng)

Overview Use this command to specify a neighbor router.
Use the **no** variant of this command to disable the specific router.

Syntax `neighbor <ipv6-link-local-addr> <interface>`
`no neighbor <ipv6-link-local-addr> <interface>`

Parameter	Description
<code><ipv6-link-local-addr></code>	Specify the link-local IPv6 address (in the format X:X::X:X) of a neighboring router to exchange routing information with.
<code><interface></code>	The interface to exchange routing information over.

Mode Router Configuration

Usage Use this command to exchange non broadcast routing information. It can be used multiple times for additional neighbors.

The [passive-interface \(IPv6 RIPng\)](#) command disables sending routing updates on an interface. If you want to send routing updates only to specific neighbors, use the [passive-interface \(IPv6 RIPng\)](#) command and this **neighbor** command together.

Examples To set 2001:db8:1::1 as a neighbor via interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# neighbor 2001:db8:1::1 eth1
```

To stop having 2001:db8:1::1 as a neighbor via interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# no neighbor 2001:db8:1::1 eth1
```

Related commands [passive-interface \(IPv6 RIPng\)](#)

passive-interface (IPv6 RIPng)

Overview Use this command to enable suppression of routing updates on an interface.
Use the **no** variant of this command to disable this function.

Syntax `passive-interface <interface>`
`no passive-interface <interface>`

Parameter	Description
<code><interface></code>	The interface to suppress routing updates on.

Default Disabled

Mode Router Configuration

Examples To suppress routing updates on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# passive-interface eth1
```

To stop suppressing routing updates on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# no passive-interface eth1
```

recv-buffer-size (IPv6 RIPng)

Overview Use this command to configure the RIPng UDP (User Datagram Protocol) receive-buffer size. This should improve UDP reliability by avoiding UDP receive buffer overruns.

Use the **no** variant of this command to unset the configured RIPng UDP receive-buffer size and set it back to the system default of 196608 bits.

Syntax `recv-buffer-size <8192-2147483647>`
`no recv-buffer-size [<8192-2147483647>]`

Default The RIPng UDP receive-buffer-size is 196608 bits by default, and is reset to the default using the **no** variant of this command.

Mode Router Configuration

Examples To configure the RIPng UPD, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# recv-buffer-size 23456789
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# no recv-buffer-size 23456789
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# no recv-buffer-size
```

redistribute (IPv6 RIPng)

Overview Use this command to redistribute information from other routing protocols into RIPng.

Use the **no** variant of this command to disable the specified redistribution. The parameters **metric** and **route-map** may be used on this command, but have no effect.

Syntax `redistribute {connected|static|ospf} [metric <0-16>] [route-map <route-map>]`
`no redistribute {connected|static|ospf} [metric <0-16>] [route-map <route-map>]`

Parameter	Description
<0-16>	Optional. Specifies the metric value to be used when redistributing information. If a value is not specified, and no value is specified using the default-metric (IPv6 RIPng) command, the default is one.
<route-map>	Optional. Specifies route-map to be used to redistribute information.
connected	Redistribute from connected routes.
static	Redistribute from static routes.
ospf	Redistribute from Open Shortest Path First (OSPF).

Default By default, the RIPng metric value is set to 1.

Mode Router Configuration

Example To redistribute information from other routing protocols into RIPng, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# redistribute static route-map mymap
awplus(config-router)# redistribute static metric 8
```

Related commands [default-metric \(IPv6 RIPng\)](#)

route (IPv6 RIPng)

Overview Use this command to configure static RIPng routes.
Use the **no** variant of this command to disable this function.

Syntax `route <ipv6-addr/prefix-length>`
`no route <ipv6-addr/prefix-length>`

Parameter	Description
<code><ipv6-addr/prefix-length></code>	Specify the IPv6 Address in format <code>X:X::X:X/Prefix-Length</code> . The prefix-length is a decimal integer between 1 and 128.

Mode Router Configuration

Usage notes Use this command to add a static RIPng route. After adding the RIPng route, the route can be checked in the RIPng routing table.

Example To configure static RIPng routes, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# route 2001:db8::1/64
```

Related commands [show ipv6 rip](#)
[clear ipv6 rip route](#)

router ipv6 rip

Overview Use this global command to enter Router Configuration mode to enable a RIPng routing process.

Use the **no** variant of this command to disable the RIPng routing process.

Syntax `router ipv6 rip`
`no router ipv6 rip`

Mode Global Configuration

Example To enable a RIPng routing process, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)#
```

show debugging ipv6 rip

Overview Use this command to see what debugging is turned on for RIPng options such as: nsm debugging, RIPng event debugging, RIPng packet debugging, and RIPng nsm debugging.

For information on filtering and saving command output, see the [“Getting_Started with AlliedWare Plus” Feature Overview and Configuration_Guide](#).

Syntax `show debugging ipv6 rip`

Mode User Exec and Privileged Exec

Usage notes Use this command to display the debug status of RIPng.

Example To display the RIPng debugging status, use the following command:

```
awplus# show debugging ipv6 rip
```


show ipv6 prefix-list

Overview Use this command to display the prefix-list entries.
Note that this command is valid for RIPng and BGP4+ routing protocols only.

Syntax `show ipv6 prefix-list [<name>|detail|summary]`

Parameter	Description
<name>	Specify the name of an individual IPv6 prefix list.
detail	Specify this parameter to show detailed output for all IPv6 prefix lists.
summary	Specify this parameter to show summary output for all IPv6 prefix lists.

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 prefix-list
awplus# show ipv6 prefix-list 10.10.0.98/8
awplus# show ipv6 prefix-list detail
```

Related commands [ipv6 prefix-list](#)

show ipv6 protocols rip

Overview Use this command to display RIPng process parameters and statistics.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 protocols rip`

Mode User Exec and Privileged Exec

Example To display RIPng process parameters and statistics, use the following command:

```
awplus# show ipv6 protocols rip
```

Output Figure 21-1: Example output from the **show ipv6 protocols rip** command

```
awplus#show ipv6 protocols rip
Routing Protocol is "RIPng"
  Sending updates every 30 seconds with +/-5 seconds, next due
in 6 seconds
  Timeout after 180 seconds, garbage collect after 120 seconds
  Outgoing update filter list for all interface is not set
  Incoming update filter list for all interface is not set
  Default redistribute metric is 1
  Redistributing:
  Interface
    eth1
  Routing for Networks:
    fe80::200:cdff:fe27:c086 vlan1
```

show ipv6 rip

Overview Use this command to show RIPng routes.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 rip`

Mode User Exec and Privileged Exec

Example To display RIPng routes, use the following command:

```
awplus# show ipv6 rip
```

Output Figure 21-2: Example output from the **show ipv6 rip** command:

```
awplus#show ipv6 rip
Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP
aggregated, Rcx - RIP connect suppressed, Rsx - RIP static
suppressed, C - Connected, S - Static, O - OSPF, B - BGP

   Network           Next Hop           If      Met Tag   Time
R  2001:db8:1::/48    2001:db8:2::/48    eth1     3    0    02:28
C  2001:db8:3::/48    ::                eth1     1    0
Ra 2001:db8:4::/48    --                --       1    0
...
```

Related commands [show ipv6 rip database](#)

show ipv6 rip database

Overview Use this command to display information about the RIPng database.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 rip database [full]`

Parameter	Description
full	Display all IPv6 RIPng full database entries including sub-optimal routes.

Mode User Exec and Privileged Exec

Example To display information about the RIPng database, use the following command:

```
awplus# show ipv6 rip database
```

Output Figure 21-3: Example output from the **show ipv6 rip database** command:

Codes: R - RIP, Rc - RIP connected, Rs - RIP static, Ra - RIP aggregated, Rcx - RIP connect suppressed, Rsx - RIP static suppressed, C - Connected, S - Static, O - OSPF, B - BGP						
	Network	Next Hop	If	Met	Tag	Time
R	2001:db8:1::/48	2001:db8:2::/48	eth1	3	0	02:28
C	2001:db8:3::/48	::	eth1	1	0	
Ra	2001:db8:4::/48		--	1	0	
...						

Related commands [show ipv6 rip](#)

show ipv6 rip interface

Overview Use this command to display information about the RIPng interfaces. You can specify an interface name to display information about a specific interface.

For information on filtering and saving command output, see the [“Getting_Started with AlliedWare Plus” Feature Overview and Configuration_Guide](#).

Syntax `show ipv6 rip interface [<interface>]`

Parameter	Description
<interface>	The interface to display information about.

Mode User Exec and Privileged Exec

Example To display RIPng interface information, use the following command:

```
awplus# show ipv6 rip interface
```

Output Figure 21-4: Example output from the **show ipv6 rip interface** command

```
lo is up, line protocol is up
RIPng is not enabled on this interface
eth1 is up, line protocol is up
Routing Protocol: RIPng
Passive interface: Disabled
Split horizon: Enabled with Poisoned Reversed
IP interface address:
2001:db8:1::1/64
2001:db8:1::2/64
...
```

timers (IPv6 RIPng)

Overview Use this command to adjust the RIPng routing network timers.

Use the **no** variant of this command to restore the defaults.

Syntax `timers basic <update> <timeout> <garbage>`
`no timers basic`

Parameter	Description
<code><update></code>	<code><5-2147483647></code> Specifies the RIPng routing table update timer in seconds. The default is 30 seconds.
<code><timeout></code>	<code><5-2147483647></code> Specifies the RIPng routing information timeout timer in seconds. The default is 180 seconds. After this interval has elapsed and no updates for a route are received, the route is declared invalid.
<code><garbage></code>	<code><5-2147483647></code> Specifies the RIPng routing garbage collection timer in seconds. The default is 120 seconds.

Default The default RIPng routing table update timer default is 30 seconds, the default RIPng routing information timeout timer is 180 seconds, and the default RIPng routing garbage collection timer is 120 seconds. The **no** variant of this command restores the default RIPng routing timers.

Mode Router Configuration

Example To adjust the RIPng routing network timers, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 rip
awplus(config-router)# timers basic 30 180 120
```

undebg ipv6 rip

Overview Use this command to disable debugging options of RIPng events, RIPng packets, and communication between RIPng and NSM processes.

Syntax `undebg ipv6 rip [all|events|nsm|packet [recv|send][detail]]`

Parameter	Description
all	Disables all RIPng debugging.
events	Disable the display of RIPng events information.
nsm	Disable the display of RIPng and NSM communication.
packet	Disable debugging of specified RIPng packets only.
recv	Disable the display of information for received packets.
send	Disable the display of information for sent packets.
detail	Disable the display of detailed information for sent or received packets.

Mode Privileged Exec and Global Configuration

Example To disable debugging options, use the following command:

```
awplus# undebg ipv6 rip events
awplus# undebg ipv6 rip all
awplus# undebg ipv6 rip packet send
awplus# undebg ipv6 rip packet recv detail
```

Related commands [debug ipv6 rip](#)

22

OSPF Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure OSPF. For more information, see the [OSPF Feature Overview and Configuration Guide](#).

- Command List**
- ["area default-cost"](#) on page 727
 - ["area authentication"](#) on page 728
 - ["area filter-list"](#) on page 729
 - ["area nssa"](#) on page 730
 - ["area range"](#) on page 732
 - ["area stub"](#) on page 734
 - ["area virtual-link"](#) on page 735
 - ["auto-cost reference bandwidth"](#) on page 738
 - ["bandwidth"](#) on page 740
 - ["capability opaque"](#) on page 741
 - ["capability restart"](#) on page 742
 - ["clear ip ospf process"](#) on page 743
 - ["compatible rfc1583"](#) on page 744
 - ["debug ospf events"](#) on page 745
 - ["debug ospf ifsm"](#) on page 746
 - ["debug ospf lsa"](#) on page 747
 - ["debug ospf n fsm"](#) on page 748
 - ["debug ospf nsm"](#) on page 749
 - ["debug ospf packet"](#) on page 750

- [“debug ospf route”](#) on page 751
- [“default-information originate”](#) on page 752
- [“default-metric \(OSPF\)”](#) on page 753
- [“distance \(OSPF\)”](#) on page 754
- [“distribute-list \(OSPF\)”](#) on page 756
- [“enable db-summary-opt”](#) on page 758
- [“host area”](#) on page 759
- [“ip ospf authentication”](#) on page 760
- [“ip ospf authentication-key”](#) on page 761
- [“ip ospf cost”](#) on page 762
- [“ip ospf database-filter”](#) on page 763
- [“ip ospf dead-interval”](#) on page 764
- [“ip ospf disable all”](#) on page 765
- [“ip ospf hello-interval”](#) on page 766
- [“ip ospf message-digest-key”](#) on page 767
- [“ip ospf mtu”](#) on page 769
- [“ip ospf mtu-ignore”](#) on page 770
- [“ip ospf network”](#) on page 771
- [“ip ospf priority”](#) on page 772
- [“ip ospf resync-timeout”](#) on page 773
- [“ip ospf retransmit-interval”](#) on page 774
- [“ip ospf transmit-delay”](#) on page 775
- [“max-concurrent-dd”](#) on page 776
- [“maximum-area”](#) on page 777
- [“neighbor \(OSPF\)”](#) on page 778
- [“network area”](#) on page 779
- [“ospf abr-type”](#) on page 781
- [“ospf restart grace-period”](#) on page 782
- [“ospf restart helper”](#) on page 783
- [“ospf router-id”](#) on page 785
- [“overflow database”](#) on page 786
- [“overflow database external”](#) on page 787
- [“passive-interface \(OSPF\)”](#) on page 788
- [“redistribute \(OSPF\)”](#) on page 789
- [“restart ospf graceful”](#) on page 791

- ["router ospf"](#) on page 792
- ["router-id"](#) on page 793
- ["show debugging ospf"](#) on page 794
- ["show ip ospf"](#) on page 795
- ["show ip ospf border-routers"](#) on page 798
- ["show ip ospf database"](#) on page 799
- ["show ip ospf database asbr-summary"](#) on page 801
- ["show ip ospf database external"](#) on page 802
- ["show ip ospf database network"](#) on page 804
- ["show ip ospf database nssa-external"](#) on page 805
- ["show ip ospf database opaque-area"](#) on page 807
- ["show ip ospf database opaque-as"](#) on page 808
- ["show ip ospf database opaque-link"](#) on page 809
- ["show ip ospf database router"](#) on page 810
- ["show ip ospf database summary"](#) on page 812
- ["show ip ospf interface"](#) on page 815
- ["show ip ospf neighbor"](#) on page 816
- ["show ip ospf route"](#) on page 818
- ["show ip ospf virtual-links"](#) on page 819
- ["show ip protocols ospf"](#) on page 820
- ["summary-address"](#) on page 821
- ["timers spf exp"](#) on page 822
- ["undebug ospf events"](#) on page 823
- ["undebug ospf ifsm"](#) on page 824
- ["undebug ospf lsa"](#) on page 825
- ["undebug ospf nfsm"](#) on page 826
- ["undebug ospf nsm"](#) on page 827
- ["undebug ospf packet"](#) on page 828
- ["undebug ospf route"](#) on page 829

area default-cost

Overview This command specifies a cost for the default summary route sent into a stub or NSSA area.

The **no** variant of this command removes the assigned default-route cost.

Syntax `area <area-id> default-cost <0-16777215>`
`no area <area-id> default-cost`

Parameter	Description
<area-id>	The OSPF area that you are specifying the default summary route cost for. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format.
	<ip-addr> OSPF Area ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295> OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.
default-cost	Indicates the cost for the default summary route used for a stub or NSSA area. Default: 1

Mode Router Configuration

Usage The default-cost option provides the metric for the summary default route, generated by the area border router, into the NSSA or stub area. Use this option only on an area border router that is attached to the NSSA or stub area. Refer to the RFC 3101 for information on NSSA.

Example To set the default cost to 10 in area 1 for the OSPF instance 100, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 1 default-cost 10
```

Related commands [area nssa](#)
[area stub](#)

area authentication

Overview Use this command to enable authentication for an OSPF area. Specifying the area authentication sets the authentication to Type 1 authentication or the Simple Text password authentication (details in RFC 2328).

The **no** variant of this command removes the authentication specification for an area.

Syntax `area <area-id> authentication [message-digest]`
`no area <area-id> authentication`

Parameter	Description
<area-id>	The OSPF area that you are enabling authentication for. This can be entered in either dotted decimal format or normal decimal format.
	<ip-addr> OSPF Area ID expressed in IPv4 address, entered in the form A.B.C.D.
	<0-4294967295> OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area OSPF Area ID.
message-digest	Enables MD5 authentication in the OSPF area.

Default By default, no authentication occurs.

Mode Router Configuration

Usage All OSPF packets transmitted in this **area** must have the same password in their OSPF header. This ensures that only routers that have the correct password may join the routing domain.

Give all routers that are to communicate with each other through OSPF the same authentication password.

Use the [ip ospf authentication-key](#) command to specify a Simple Text password.
Use the [ip ospf message-digest-key](#) command to specify MD5 password.

Example `awplus# configure terminal`
`awplus(config)# router ospf 100`
`awplus(config-router)# area 1 authentication`

Related commands [ip ospf authentication](#)
[ip ospf message-digest-key](#)

area filter-list

Overview This command configures filters to advertise summary routes on Area Border Routers (ABR).

This command is used to suppress particular intra-area routes from/to an area to/from the other areas. You can use this command in conjunction with the prefix-list command.

The **no** variant of this command removes the filter configuration.

Syntax `area <area-id> filter-list prefix <prefix-list> {in|out}`
`no area <area-id> filter-list prefix <prefix-list> {in|out}`

Parameter	Description
<area-id>	The OSPF area that you are configuring the filter for. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format.
	<ip-addr> OSPF Area ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295> OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.
prefix	Use prefix-list to filter summary.
<prefix-list>	Name of a prefix-list.
in	Filter routes from the other areas to this area.
out	Filter routes from this area to the other areas.

Mode Router Configuration

area nssa

Overview This command sets an area as a Not-So-Stubby-Area (NSSA). By default, no NSSA area is defined.

Use this command to simplify administration if you are connecting a central site using OSPF to a remote site that is using a different routing protocol. You can extend OSPF to cover the remote connection by defining the area between the central router and the remote router as an NSSA.

There are no external routes in an OSPF stub area, so you cannot redistribute from another protocol into a stub area. A NSSA allows external routes to be flooded within the area. These routes are then leaked into other areas. Although, the external routes from other areas still do not enter the NSSA. You can either configure an area to be a stub area or an NSSA, not both.

The **no** variant of this command removes this designation.

Syntax `area <area-id> nssa [default-information-originate <metric> | no-redistribution | no-summary | translator-role <role> ]`
`no area <area-id> nssa [default-information-originate | no-redistribution | no-summary | translator-role ]`

Parameter	Description				
<area-id>	The OSPF area that you are configuring as an NSSA. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format. <table> <tr> <td><ip-addr></td><td>OSPF Area ID expressed in IPv4 address format A.B.C.D.</td></tr> <tr> <td><0-4294967295></td><td>OSPF Area ID expressed as a decimal number within the range shown.</td></tr> </table> For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.	<ip-addr>	OSPF Area ID expressed in IPv4 address format A.B.C.D.	<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.
<ip-addr>	OSPF Area ID expressed in IPv4 address format A.B.C.D.				
<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.				
default-information-originate	Originate Type-7 default LSA into NSSA.				
<metric>	The external or internal metric. Specify the following: <table> <tr> <td>metric<0-16777214></td><td>The metric value.</td></tr> <tr> <td>metric-type<1-2></td><td>External metric type.</td></tr> </table>	metric<0-16777214>	The metric value.	metric-type<1-2>	External metric type.
metric<0-16777214>	The metric value.				
metric-type<1-2>	External metric type.				
no-redistribution	Do not redistribute external route into NSSA.				
no-summary	Do not inject inter-area route into NSSA.				
translator-role	Specify NSSA-ABR translator-role.				

Parameter	Description	
<role>	The role type. Specify one of the following keywords:	
	always	Router always translate NSSA-LSA to Type-5 LSA.
	candidate	Router may translate NSSA-LSA to Type-5 LSA if it is elected.
	never	Router never translate NSSA-LSA.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 0.0.0.51 nssa
awplus(config-router)# area 3 nssa translator-role candidate
no-redistribution default-information-originate metric 34
metric-type 2
```

Related commands [area default-cost](#)

area range

Overview Use this command to summarize OSPF routes at an area boundary, configuring an IPv4 address range which consolidates OSPF routes. By default, this feature is not enabled.

A summary route created by this command is then advertised to other areas by the Area Border Routers (ABRs). In this way, routing information is condensed at area boundaries and outside the area so that routes are exchanged between areas in an efficient manner.

If the network numbers in an area are arranged into sets of contiguous routes, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

Use the cost parameter to specify a metric that will be advertised in the summary Link State Advertisement (LSA), rather than relying on the standard method to calculate the metric for the LSA.

The **no** variant of this command disables this function and restores default behavior.

Syntax `area <area-id> range <ip-addr/prefix-length> [advertise] [cost <0-16777215>]`

`area <area-id> range <ip-addr/prefix-length> not-advertise`

`no area <area-id> range <ip-addr/prefix-length>`

Parameter	Description
<area-id>	The OSPF area that you summarizing the routes for. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format.
	<ip-addr> OSPF Area ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295> OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.
<ip-addr/prefix-length>	The area range prefix and length.
advertise	Advertise this range as a summary route into other areas.

Parameter	Description
not-advertise	Does not advertise this range.
cost	Optionally override the metric that would normally be calculated for this summary with a user-defined cost to be advertised for this summary LSA. Specify the metric to be advertised for this route in the range 0-16777215.

Default The area range is not configured by default. The area range is advertised if it is configured.

Mode Router Configuration

Usage notes You can configure multiple ranges on a single area with multiple instances of this command, so OSPF summarizes addresses for different sets of IPv4 address ranges. Ensure OSPF IPv4 routes exist in the area range for advertisement before using this command.

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 1 range 192.16.0.0/16
awplus(config-router)# area 1 range 203.18.0.0/16 cost 70
```

To remove a cost configured on an area range, re-enter the area range without the optional cost parameter. This will set the metric calculation back to the default algorithm.

```
awplus(config-router)# area 1 range 207.14.0.0/16 cost 35
awplus(config-router)# area 1 range 207.14.0.0/16
```

Command changes Version 5.5.0-0.1: parameter **cost** added

area stub

Overview This command defines an OSPF area as a stub area. By default, no stub area is defined.

Use this command when routers in the area do not require learning about summary LSAs from other areas. You can define the area as a totally stubby area by configuring the Area Border Router of that area using the **area stub no-summary** command.

There are two stub area router configuration commands: the **area stub** and **area default-cost** commands. In all routers attached to the stub area, configure the area by using the **area stub** command. For an area border router (ABR) attached to the stub area, also use the **area default-cost** command.

The **no** variant of this command removes this definition.

Syntax `area <area-id> stub [no-summary]`
`no area <area-id> stub [no-summary]`

Parameter	Description
<area-id>	The OSPF area that you are configuring as a stub area. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format. For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.
	<ip-addr> OSPF Area ID expressed in IPv4 address in the format A.B.C.D.
	<0-4294967295> OSPF Area ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.
no-summary	Stops an ABR from sending summary link advertisements into the stub area.

Mode Router Configuration

Example `awplus# configure terminal`
`awplus(config)# router ospf 100`
`awplus(config-router)# area 1 stub`

Related commands [area default-cost](#)

area virtual-link

Overview This command configures a link between two backbone areas that are physically separated through other non-backbone areas.

In OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection.

The **no** variant of this command removes the virtual link.

Syntax

```
area <area-id> virtual-link <ip-addr> [<auth-key>|<msg-key>]
no area <area-id> virtual-link <ip-addr> [<auth-key>|<msg-key>]

area <area-id> virtual-link <ip-addr> authentication
[message-digest|null] [<auth-key>|<msg-key>]

no area <area-id> virtual-link <ip-addr> authentication
[message-digest|null] [<auth-key>|<msg-key>]

area <area-id> virtual-link <ip-addr> [authentication]
[dead-interval <1-65535>] [hello-interval <1-65535>]
[retransmit-interval <1-3600>] [transmit-delay <1-3600>]

no area <area-id> virtual-link <ip-addr> [authentication]
[dead-interval] [hello-interval] [retransmit-interval]
[transmit-delay]
```

Parameter	Description				
<area-id>	The area ID of the transit area that the virtual link passes through. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format. <table> <tr> <td><ip-addr></td><td>OSPF Area ID expressed in IPv4 address format A.B.C.D.</td></tr> <tr> <td><0-4294967295></td><td>OSPF Area ID expressed as a decimal number within the range shown.</td></tr> </table> For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area ID.	<ip-addr>	OSPF Area ID expressed in IPv4 address format A.B.C.D.	<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.
<ip-addr>	OSPF Area ID expressed in IPv4 address format A.B.C.D.				
<0-4294967295>	OSPF Area ID expressed as a decimal number within the range shown.				
<ip-addr>	The OSPF router ID of the virtual link neighbor.				
<auth-key>	Specifies the password used for this virtual link. Use the format: authentication-key<pswd-short> <table> <tr> <td><pswd-short></td><td>An 8 character password.</td></tr> </table>	<pswd-short>	An 8 character password.		
<pswd-short>	An 8 character password.				
<msg-key>	Specifies a message digest key using the MD5 encryption algorithm. Use the following format: message-digest-key<1-255> md5 <pswd-long> <table> <tr> <td><1-255></td><td>The key ID.</td></tr> <tr> <td><pswd-long></td><td>Authentication password of 16 characters.</td></tr> </table>	<1-255>	The key ID.	<pswd-long>	Authentication password of 16 characters.
<1-255>	The key ID.				
<pswd-long>	Authentication password of 16 characters.				
authentication	Enables authentication on this virtual link.				

Parameter	Description
message-digest	Use message-digest authentication.
null	Use null authentication to override password or message digest.
dead-interval	If no packets are received from a particular neighbor for dead-interval seconds, the router considers that neighboring router as being off-line. Default: 40 seconds
	<1-65535> The number of seconds in the interval.
hello-interval	The interval the router waits before it sends a hello packet. Default: 10 seconds
	<1-65535> The number of seconds in the interval.
retransmit-interval	The interval the router waits before it retransmits a packet. Default: 5 seconds
	<1-3600> The number of seconds in the interval.
transmit-delay	The interval the router waits before it transmits a packet. Default: 1 seconds
	<1-3600> The number of seconds in the interval.

Mode Router Configuration

Usage notes You can configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these two routers, joined by a virtual link, as if they were connected by an unnumbered point-to-point network. To configure a virtual link, you require:

- The transit area ID, i.e. the area ID of the non backbone area that the two backbone routers are both connected to.
- The corresponding virtual link neighbor's router ID. To see the router ID use the [show ip ospf](#) command.

Configure the **hello-interval** to be the same for all routers attached to a common network. A short **hello-interval** results in the router detecting topological changes faster but also an increase in the routing traffic.

The **retransmit-interval** is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The **transmit-delay** is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet are incremented by this amount. Set the **transmit-delay** to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

Example To configure a virtual link, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# area 1 virtual-link 10.10.11.50
hello-interval 5 dead-interval 10
```

Related commands

- area authentication
- show ip ospf
- show ip ospf virtual-links

auto-cost reference bandwidth

Overview This command controls how OSPF calculates default metrics for the interface. Use the **no** variant of this command to assign cost based only on the interface bandwidth.

Syntax `auto-cost reference-bandwidth <1-4294967>`
`no auto-cost reference-bandwidth`

Parameter	Description
<code><1-4294967></code>	The reference bandwidth in terms of Mbits per second (Mbps).

Default 1000 Mbps

Usage notes By default, OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the interface bandwidth. The default for the reference bandwidth is 1000 Mbps. As a result, if this default is used, there is very little difference between the metrics applied to interfaces of increasing bandwidth beyond 1000 Mbps.

The auto-cost command is used to alter this reference bandwidth in order to give a real difference between the metrics of high bandwidth links of differing bandwidths. In a network that has multiple links with high bandwidths, specify a larger reference bandwidth value to differentiate the costs on those links.

Cost is calculated by dividing the reference bandwidth (Mbps) by the layer 3 interface (Switched Virtual Interface (SVI), Loopback or Ethernet interface) bandwidth. Interface bandwidth may be altered by using the [bandwidth](#) command as the SVI does not auto detect the bandwidth based on the speed of associated switch ports.

When the reference bandwidth calculation results in a cost integer greater than 1 but contains a fractional value (value after the decimal point), the result rounds down to the nearest integer. The following example shows how the cost is calculated.

The reference bandwidth is 1000 Mbps and the interface bandwidth is 7 Mbps.

Calculation = $1000/7$

Calculation result = 142.85 (integer of 142, fractional value of 0.85)

Result after rounding down to the nearest integer = 142 (Interface cost is 142)

When the reference bandwidth calculation results in a cost less than 1, it is rounded up to the nearest integer which is 1. The following example shows how the cost is calculated.

The reference bandwidth is 1000 Mbps and the interface bandwidth is 10000 Mbps.

Calculation = $1000/10000$

Calculation result = 0.1

Result after rounding up to the nearest integer = 1 (Interface cost is 1)

The auto-cost reference bandwidth value should be consistent across all OSPF routers in the OSPF process.

Note that using the `ip ospf cost` command on a layer 3 interface will override the cost calculated by this command.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# auto-cost reference-bandwidth 1000
```

Related commands `ip ospf cost`

bandwidth

Overview Use this command to specify the maximum bandwidth to be used for each interface. The bandwidth value is in bits per second. OSPF uses this to calculate metrics for the interface.

The **no** variant of this command removes any applied bandwidth value.

Syntax `bandwidth <bandwidth-setting>`
`no bandwidth`

Parameter	Description
<code><bandwidth-setting></code>	Sets the bandwidth for the interface. Enter a value in the range 1 to 10000000000 bits per second. Note that to avoid entering many zeros, you can add k, m, or g to internally add 3, 6 or 9 zeros to the number entered. For example entering 1k is the same as entering 1000.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Example To set the bandwidth on eth1 to be 10 Mbps, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# bandwidth 10000000
or
awplus(config-if)# bandwidth 10m
```

Related commands [show interface](#)

capability opaque

Overview This command enables opaque-LSAs. Opaque-LSAs are Type 9, 10 and 11 LSAs that deliver information used by external applications.

Use the **no** variant of this command to disable opaque-LSAs.

Syntax `capability opaque`
`no capability opaque`

Default By default, opaque-LSAs are enabled.

Mode Router Configuration

Example `awplus# configure terminal`
`awplus(config)# router ospf 100`
`awplus(config-router)# no capability opaque`

capability restart

Overview This command enables OSPF Graceful Restart or restart signaling features. By default, this is enabled.

Use the **no** variant of this command to disable OSPF Graceful Restart and restart signaling features.

Syntax `capability restart [graceful|signaling]`
`no capability restart`

Parameter	Description
graceful	Enable graceful OSPF restart.
signaling	Enable OSPF restart signaling.

Default Graceful restart

Mode Router Configuration

Example `awplus# configure terminal`
`awplus(config)# router ospf 100`
`awplus(config-router)# capability restart graceful`

clear ip ospf process

Overview This command clears and restarts the OSPF routing process. Specify the Process ID to clear one particular OSPF process. When no Process ID is specified, this command clears all running OSPF processes.

Syntax `clear ip ospf [<0-65535>] process`

Parameter	Description
<0-65535>	The Routing Process ID.

Mode Privileged Exec

Example `awplus# clear ip ospf process`

compatible rfc1583

Overview This command changes the method used to calculate summary route to the that specified in RFC 1583. By default, OSPF uses the method specified in RFC 2328.

RFC 1583 specifies a method for calculating the metric for summary routes based on the minimum metric of the component paths available. RFC 2328 specifies a method for calculating metrics based on maximum cost.

It is possible that some ABRs in an area might conform to RFC 1583 and others support RFC 2328, which could lead to incompatibility in their interoperation. This command addresses this issue by allowing you to selectively disable compatibility with RFC 2328.

Use the **no** variant of this command to disable RFC 1583 compatibility.

Syntax `compatible rfc1583`
`no compatible rfc1583`

Mode Router Configuration

Example `awplus# configure terminal`
`awplus(config)# router ospf 100`
`awplus(config-router)# compatible rfc1583`

debug ospf events

Overview This command enables OSPF debugging for OSPF event troubleshooting.

To enable all debugging options, specify **debug ospf event** with no additional parameters.

The **no** and **undebug** variant of this command disable OSPF debugging. Use this command without parameters to disable all the options.

Syntax `debug ospf events [abr] [asbr] [lsa] [nssa] [os] [router]
[vlink]`
`no debug ospf events [abr] [asbr] [lsa] [nssa] [os] [router]
[vlink]`

Parameter	Description
abr	Shows ABR events.
asbr	Shows ASBR events.
lsa	Shows LSA events.
nssa	Shows NSSA events.
os	Shows OS interaction events.
router	Shows other router events.
vlink	Shows virtual link events.

Mode Privileged Exec and Global Configuration

Example `awplus# debug ospf events asbr lsa`

Related commands [terminal monitor](#)
[undebug ospf events](#)

debug ospf ifsm

- Overview** This command specifies debugging options for OSPF Interface Finite State Machine (IFSM) troubleshooting.
- To enable all debugging options, specify **debug ospf ifsm** with no additional parameters.
- The **no** and **undebug** variant of this command disable OSPF IFSM debugging. Use this command without parameters to disable all the options.

Syntax `debug ospf ifsm [status] [events] [timers]`
`no debug ospf ifsm [status] [events] [timers]`

Parameter	Description
events	Displays IFSM event information.
status	Displays IFSM status information.
timers	Displays IFSM timer information.

Mode Privileged Exec and Global Configuration

Example `awplus# no debug ospf ifsm events status`
`awplus# debug ospf ifsm status`
`awplus# debug ospf ifsm timers`

Related commands [terminal monitor](#)
[undebug ospf ifsm](#)

debug ospf lsa

Overview This command enables debugging options for OSPF Link State Advertisements (LSA) troubleshooting. This displays information related to internal operations of LSAs.

To enable all debugging options, specify **debug ospf lsa** with no additional parameters.

The **no** and **undebug** variant of this command disable OSPF LSA debugging. Use this command without parameters to disable all the options.

Syntax

```
debug ospf lsa [flooding] [generate] [install] [maxage] [refresh]
no debug ospf lsa [flooding] [generate] [install] [maxage] [refresh]
```

Parameter	Description
flooding	Displays LSA flooding.
generate	Displays LSA generation.
install	Show LSA installation.
maxage	Shows maximum age of the LSA in seconds.
refresh	Displays LSA refresh.

Mode Privileged Exec and Global Configuration

Examples awplus# undebug ospf lsa refresh

Output Figure 22-1: Example output from the **debug ospf lsa** command

```
2002/05/09 14:08:11 OSPF: LSA[10.10.10.10:10.10.10.70]: instance(0x8139cd0)
created with Link State Update
2002/05/09 14:08:11 OSPF: RECV[LS-Upd]: From 10.10.10.70 via vlan5:10.10.10.50
(10.10.10.10 -> 224.0.0.5)
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: Begin send queue
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: # of LSAs 1, destination 224.0.0.5
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: End send queue
2002/05/09 14:12:33 OSPF: SEND[LS-Upd]: To 224.0.0.5 via vlan5:10.10.10.50
```

Related commands [terminal monitor](#)
[undebug ospf lsa](#)

debug ospf nfsm

- Overview** This command enables debugging options for OSPF Neighbor Finite State Machines (NFSMs).
- To enable all debugging options, specify **debug ospf nfsm** with no additional parameters.
- The **no** and **undebug** variant of this command disable OSPF NFSM debugging. Use this command without parameters to disable all the options.

Syntax `debug ospf nfsm [events] [status] [timers]`
`no debug ospf nfsm [events] [status] [timers]`

Parameter	Description
events	Displays NFSM event information.
status	Displays NFSM status information.
timers	Displays NFSM timer information.

Mode Privileged Exec and Global Configuration

Examples `awplus# debug ospf nfsm events`
`awplus# no debug ospf nfsm timers`
`awplus# undebug ospf nfsm events`

Related commands [terminal monitor](#)
[undebug ospf nfsm](#)

debug ospf nsm

Overview This command enables debugging options for the OSPF Network Service Module. To enable both debugging options, specify **debug ospf nsm** with no additional parameters. The **no** and **undebug** variant of this command disable OSPF NSM debugging. Use this command without parameters to disable both options.

Syntax debug ospf nsm [interface] [redistribute]
no debug ospf nsm [interface] [redistribute]

Parameter	Description
interface	Specify NSM interface information.
redistribute	Specify NSM redistribute information.

Mode Privileged Exec and Global Configuration

Examples awplus# debug ospf nsm interface
awplus# no debug ospf nsm redistribute
awplus# undebug ospf nsm interface

Related commands [terminal monitor](#)
[undebug ospf nsm](#)

debug ospf packet

Overview This command enables debugging options for OSPF packets.

To enable all debugging options, specify **debug ospf packet** with no additional parameters.

The **no** and **undebug** variant of this command disable OSPF packet debugging. Use this command without parameters to disable all options.

Syntax debug ospf packet [dd] [detail] [hello] [ls-ack] [ls-request] [ls-update] [recv] [send]

no debug ospf packet [dd] [detail] [hello] [ls-ack] [ls-request] [ls-update] [recv] [send]

Parameter	Description
dd	Specifies debugging for OSPF database descriptions.
detail	Sets the debug option to detailed information.
hello	Specifies debugging for OSPF hello packets.
ls-ack	Specifies debugging for OSPF link state acknowledgments.
ls-request	Specifies debugging for OSPF link state requests.
ls-update	Specifies debugging for OSPF link state updates.
recv	Specifies the debug option set for received packets.
send	Specifies the debug option set for sent packets.

Mode Privileged Exec and Global Configuration

Examples awplus# debug ospf packet detail

awplus# debug ospf packet dd send detail

awplus# no debug ospf packet ls-request recv detail

awplus# undebug ospf packet ls-request recv detail

Related commands [terminal monitor](#)

[undebug ospf packet](#)

debug ospf route

- Overview** This command enables debugging of route calculation. Use this command without parameters to turn on all the options.
- To enable all debugging options, specify **debug ospf route** with no additional parameters.
- The **no** and **undebug** variant of this command disable OSPF route debugging. Use this command without parameters to disable all options.

Syntax debug ospf route [ase] [ia] [install] [spf]
no debug ospf route [ase] [ia] [install] [spf]

Parameter	Description
ia	Specifies the debugging of Inter-Area route calculation.
ase	Specifies the debugging of external route calculation.
install	Specifies the debugging of route installation.
spf	Specifies the debugging of SPF calculation.

Mode Privileged Exec and Global Configuration

Examples awplus# debug ospf route
awplus# no debug ospf route ia
awplus# debug ospf route install
awplus# undebug ospf route install

Related commands [terminal monitor](#)
[undebug ospf route](#)

default-information originate

Overview This command creates a default external route into an OSPF routing domain.

When you use the **default-information originate** command to redistribute routes into an OSPF routing domain, then the system acts like an Autonomous System Boundary Router (ASBR). By default, an ASBR does not generate a default route into the OSPF routing domain.

When using this command, also specify the **route-map <route-map>** option to avoid a dependency on the default network in the routing table.

The **metric-type** is an external link type associated with the default route advertised into the OSPF routing domain. The value of the external route could be either Type 1 or 2. The default is Type 2.

The **no** variant of this command disables this feature.

Syntax

```
default-information originate [always] [metric <metric>]
[metric-type <1-2>] [route-map <route-map>]

no default-information originate [always] [metric]
[metric-type] [route-map]
```

Parameter	Description
always	Used to advertise the default route regardless of whether there is a default route.
<metric>	The metric value used in creating the default route. Enter a value in the range 0 to 16777214. The default metric value is 10. The value used is specific to the protocol.
<1-2>	External metric type for default routes, either OSPF External Type 1 or Type 2 metrics. Enter the value 1 or 2.
route-map	Specifies to use a specific route-map.
<route-map>	The route-map name. It is a string comprised of any characters, numbers or symbols.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# default-information originate always
metric 23 metric-type 2 route-map myinfo
```

Related commands [route-map](#)

default-metric (OSPF)

Overview This command sets default metric values for the OSPF routing protocol.

The **no** variant of this command returns OSPF to using built-in, automatic metric translations, as appropriate for each routing protocol.

Syntax `default-metric <1-16777214>`
`no default-metric [<1-16777214>]`

Parameter	Description
<code><1-16777214></code>	Default metric value appropriate for the specified routing protocol.

Mode Router Configuration

Usage notes A default metric facilitates redistributing routes even with incompatible metrics. If the metrics do not convert, the default metric provides an alternative and enables the redistribution to continue. The effect of this command is that OSPF will use the same metric value for **all** redistributed routes. Use this command in conjunction with the [redistribute \(OSPF\)](#) command.

Examples

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# default-metric 100
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# no default-metric
```

Related commands [redistribute \(OSPF\)](#)

distance (OSPF)

Overview This command sets the administrative distance for OSPF routes based on the route type. Your device uses this value to select between two or more routes to the same destination from two different routing protocols. The route with the smallest administrative distance value is added to the Forwarding Information Base (FIB). See the [Route_Selection Feature Overview and Configuration Guide](#) for more information.

Use the command **distance ospf** to set the distance for an entire category of OSPF routes, rather than the specific routes that pass an access list.

Use the command **distance <1-255>**, with no other parameter, to set the same distance for all OSPF route types.

The **no** variant of this command sets the administrative distance for all OSPF routes to the default of 110.

Syntax

```
distance <1-255>
distance ospf {external <1-255>|inter-area <1-255>|intra-area <1-255>}
no distance {ospf|<1-255>}
```

Parameter	Description
<1-255>	Specify the Administrative Distance value for OSPF routes.
external	Sets the distance for routes from other routing domains, learned by redistribution. Specify an OSPF external distance in the range <1-255>.
inter-area	Sets the distance for all routes from one area to another area. Specify an OSPF inter-area distance in the range <1-255>.
intra-area	Sets the distance for all routes within an area. Specify an OSPF intra-area distance in the range <1-255>.

Default The default OSPF administrative distance is 110. The default Administrative Distance for each type of route (intra, inter, or external) is 110.

Mode Router Configuration

Usage notes The administrative distance rates the trustworthiness of a routing information source. The distance could be any integer from 0 to 255. A higher distance value indicates a lower trust rating. For example, an administrative distance of 255 indicates that the routing information source cannot be trusted and should be ignored.

Use this command to set the distance for an entire group of routes, rather than a specific route that passes an access list.

Examples To set the following administrative distances for route types in OSPF 100:

- 20 for inter-area routes

- 10 for intra-area routes
- 40 for external routes

use the commands:

```
awplus(config)# router ospf 100
```

```
awplus(config-router)# distance ospf inter-area 20 intra-area  
10 external 40
```

To set the administrative distance for all routes in OSPF 100 back to the default of 110, use the commands:

```
awplus(config)# router ospf 100
```

```
awplus(config-router)# no distance ospf
```

distribute-list (OSPF)

Overview Use this command to apply filtering to the transfer of routing information between OSPF and the IP route table. You can apply filtering from OSPF to the IP route table using an **in** distribute-list.

The effect of an **in** filter is that some route information that OSPF has learned from LSA updates will not be installed into the IP route table.

The entities that are used to perform filtering are route-maps, which match on certain attributes in the routes that are being transferred.

For information about route maps, see the [Routemaps Feature Overview and Configuration Guide](#).

The **no** variant of this command removes the configured distribute-list command entry.

Syntax `distribute-list route-map <route-map-name> in`
`no distribute-list route-map <route-map-name> in`

Parameter	Description
<code><route-map-name></code>	The name of the route-map.
<code>in</code>	Indicates that this applies to incoming advertised routes.

Mode Router Configuration

Usage notes The **in** distribute-lists carry out the following route filtering activities:

- The **in** distribute list is applied to the process of installing OSPF routes into the IP route table. The SPF calculations generate a set of routes calculated from the LSA database. By default, all of these routes become OSPF's candidate routes for inclusion into the IP route table.
- An **in** distribute-list can be used to control whether or not certain routes generated by the SPF calculation are included into the set of candidates for inclusion into the IP route table. Those routes that match **deny** entries in the distribute-list will not be considered for inclusion into the IP route table.

Examples The following example shows the installation of OSPF routes into the IP route table with route map "mymap1" applied, which will process routes that have been tagged 100:

```
awplus# configure terminal
awplus(config)# route-map mymap1 permit 10
awplus(config-route-map)# match tag 100
awplus(config-route-map)# exit
awplus(config)# router ospf 100
awplus(config-router)# distribute-list route-map mymap1 in
```


Use the following commands to configure a route-map to specifically prevent OSPF from offering 192.168.1.0/24 as a candidate for inclusion into the IP route table:

```
awplus# configure terminal
awplus(config)# ip prefix-list 100 seq 5 permit 192.168.1.0/24
awplus(config)# route-map 100 deny 10
awplus(config-route-map)# match ip address prefix-list 100
awplus(config-route-map)# exit
awplus(config)# route-map 100 permit 20
awplus(config-router)# router ospf 1
awplus(config-router)# distribute-list route-map 100 in
```

Related commands

- [match interface](#)
- [redistribute \(OSPF\)](#)
- [route-map](#)

enable db-summary-opt

Overview This command enables OSPF database summary list optimization.
The **no** variant of this command disables database summary list optimization.

Syntax enable db-summary-opt
no enable db-summary-opt

Default The default setting is disabled.

Mode Router Configuration

Usage When this feature is enabled, the database exchange process is optimized by removing the LSA from the database summary list for the neighbor, if the LSA instance in the database summary list is the same as, or less recent than, the listed LSA in the database description packet received from the neighbor.

Examples To enable OSPF database summary list optimization, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf
awplus(config-router)# enable db-summary-opt
```

To disable OSPF database summary list optimization, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf
awplus(config-router)# no enable db-summary-opt
```

**Validation
Commands** [show running-config](#)

host area

Overview This command configures a stub host entry belonging to a particular area. You can use this command to advertise specific host routes in the router-LSA as stub link. Since stub host belongs to the specified router, specifying cost is optional.

The **no** variant of this command removes the host area configuration.

Syntax `host <ip-address> area <area-id> [cost <0-65535>]`
`no host <ip-address> area <area-id> [cost <0-65535>]`

Parameter	Description
<code><ip-address></code>	The IPv4 address of the host, in dotted decimal notation.
<code><area-id></code>	The OSPF area ID of the transit area that configuring the stub host entry for. Use one of the following formats: - dotted decimal format, e.g. 0.0.1.2. - normal decimal format in the range <0-4294967295>, e.g. 258.
<code>cost <0-65535></code>	The cost for the stub host entry.

Default By default, no host entry is configured.

Mode Router Configuration

Example `awplus# configure terminal`
`awplus(config)# router ospf 100`
`awplus(config-router)# host 172.16.10.100 area 1`
`awplus(config-router)# host 172.16.10.101 area 2 cost 10`

ip ospf authentication

Overview This command sets the authentication method used when sending and receiving OSPF packets on the current interface. The default is to use no authentication. If no authentication method is specified in this command, then plain text authentication will be used.

The **no** variant of this command disables the authentication.

Syntax `ip ospf [<ip-address>] authentication [message-digest|null]`
`no ip ospf [<ip-address>] authentication`

Parameter	Description
<ip-address>	The IP address of the interface.
message-digest	Use the message digest authentication.
null	Use no authentication. This overrides the password or message digest authentication of the interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes Use the [ip ospf authentication-key](#) command to specify a simple text password. Use the [ip ospf message-digest-key](#) command to specify an MD5 key.

Example To configure PPP interface ppp0 to have no authentication, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf authentication null
```

This will override any text or MD5 authentication configured on this interface.

Related commands [ip ospf authentication-key](#)
[area authentication](#)
[ip ospf message-digest-key](#)

ip ospf authentication-key

Overview This command specifies an OSPF authentication password for the neighboring routers.

The **no** variant of this command removes the OSPF authentication password.

Syntax `ip ospf [<ip-address>] authentication-key <pswd-long>`
`no ip ospf [<ip-address>] authentication-key`

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.
<pswd-long>	The authentication password. The string you enter at the end of the command line will be used.

Default No password specified

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command creates a password (key) that is inserted into the OSPF header when AlliedWare Plus™ software originates routing protocol packets. Assign a separate password to each network for different interfaces. All neighboring routers on the same network with the same password exchange OSPF routing data.

The key can be used only when authentication is enabled for an area. Use the **area authentication** command to enable authentication.

Simple password authentication allows a password to be configured for each area. Configure the routers in the same routing domain with the same password.

Example To turn on authentication in area 0 and then create an authentication key named 'very secure password' on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# network 10.10.10.0/24 area 0
awplus(config-router)# area 0 authentication
awplus(config-router)# exit
awplus(config)# interface ppp0
awplus(config-if)# ip ospf 3.3.3.3 authentication-key very
secure password
```

Related commands [area authentication](#)
[ip ospf authentication](#)

ip ospf cost

Overview This command explicitly specifies the cost of the link-state metric in a router-LSA. The **no** variant of this command resets the interface cost to the default.

Syntax `ip ospf [<ip-address>] cost <1-65535>`
`no ip ospf [<ip-address>] cost`

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.
<1-65535>	The link-state metric.

Default No static value. The OSPF cost is automatically calculated by using the [auto-cost reference bandwidth](#) command.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command explicitly sets a user specified cost of sending packets out the interface. Using this command overrides the cost value calculated automatically with the auto-cost reference bandwidth feature.

The interface cost indicates the overhead required to send packets across a certain interface. This cost is stated in the Router-LSA's link. Typically, the cost is inversely proportional to the bandwidth of an interface. By default, the cost of an interface is calculated according to the following formula:

- $\text{reference bandwidth} / \text{interface bandwidth}$

Use the **ip ospf cost** command to set the interface cost manually.

Example To set the OSPF cost to 10 on the PPP interface ppp0 for IP address 10.10.10.50, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf 10.10.10.50 cost 10
```

Related commands [show ip ospf interface](#)
[auto-cost reference bandwidth](#)

ip ospf database-filter

Overview This command turns on the LSA database-filter for a particular interface. The **no** variant of this command turns off the LSA database-filter.

Syntax `ip ospf [<ip-address>] database-filter all out`
`no ip ospf [<ip-address>] database-filter`

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.

Default All outgoing LSAs are flooded to the interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes OSPF floods new LSAs over all interfaces in an area, except the interface on which the LSA arrives. This redundancy ensures robust flooding. However, too much redundancy can waste bandwidth and might lead to excessive link and CPU usage in certain topologies, resulting in destabilizing the network. To avoid this, use the **ip ospf database-filter** command to block flooding of LSAs over specified interfaces.

Example To stop flooding new LSAs on the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if# ip ospf database-filter all out
```

ip ospf dead-interval

Overview This command sets the interval during which no hello packets are received and after which a neighbor is declared dead.

The dead-interval is the amount of time that OSPF waits to receive an OSPF hello packet from the neighbor before declaring the neighbor is down. This value is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

The **no** variant of this command returns the interval to the default of 40 seconds. If you have configured this command specifying the IP address of the interface and want to remove the configuration, specify the IP address (**no ip ospf**<ip-address>**dead-interval**).

Syntax `ip ospf [<ip-address>] dead-interval <1-65535>`
`no ip ospf [<ip-address>] dead-interval`

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.
<1-65535>	The interval in seconds. Default: 40

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Example To set the dead-interval to 10 seconds on the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf dead-interval 10
```

Related commands [ip ospf hello-interval](#)
[show ip ospf interface](#)

ip ospf disable all

Overview This command completely disables OSPF packet processing on an interface. It overrides the [network area](#) command and disables the processing of packets on the specific interface.

Use the **no** variant of this command to restore OSPF packet processing on a selected interface.

Syntax `ip ospf disable all`
`no ip ospf disable all`

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Example To disable OSPF packet processing on the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf disable all
```

ip ospf hello-interval

- Overview** This command specifies the interval between hello packets.
- The hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter hello interval ensures faster detection of topological changes, but results in more routing traffic.
- The **no** variant of this command returns the interval to the default of 10 seconds.

Syntax `ip ospf [<ip-address>] hello-interval <1-65535>`
`no ip ospf [<ip-address>] hello-interval`

Parameter	Description
<ip-address>	The IP address of the interface, in dotted decimal notation.
<1-65535>	The interval in seconds. Default: 10

Default 10 seconds

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Example To set the hello-interval to 3 seconds on the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf hello-interval 3
```

Related commands [ip ospf dead-interval](#)
[show ip ospf interface](#)

ip ospf message-digest-key

Overview This command registers an MD5 key for OSPF MD5 authentication.

Message Digest Authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a message digest that gets appended to the packet.

The **no** variant of this command removes the MD5 key.

Syntax `ip ospf [<ip-address>] message-digest-key <key-id> md5
<pswd-long>`
`no ip ospf [<ip-address>] message-digest-key <key-id>`

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.
<key-id>	A key ID number specified as an integer between 1 and 255.
md5	Use the MD5 algorithm.
<pswd-long>	The OSPF password. This is a string of 1 to 16 characters including spaces.

Default No MD5 key registered

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes Use this command for uninterrupted transitions between passwords. It allows you to add a new key without having to delete the existing key. While multiple keys exist, all OSPF packets will be transmitted in duplicate; one copy of the packet will be transmitted for each of the current keys. This is helpful for administrators who want to change the OSPF password without disrupting communication. The system begins a rollover process until all the neighbors have adopted the new password. This allows neighboring routers to continue communication while the network administrator is updating them with a new password. The router will stop sending duplicate packets once it detects that all of its neighbors have adopted the new password.

Maintain only one password per interface, removing the old password whenever you add a new one. This will prevent the local system from continuing to communicate with the system that is using the old password. Removing the old password also reduces overhead during rollover. All neighboring routers on the same network must have the same password value to enable exchange of OSPF routing data.

Examples To configure OSPF authentication on the PPP interface ppp0, with a key of 'yourpass', use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf authentication message-digest
awplus(config-if)# ip ospf message-digest-key 1 md5 yourpass
```

ip ospf mtu

Overview This command sets the MTU size for OSPF. Whenever OSPF constructs packets, it uses the interface MTU size as Maximum IP packet size. This command forces OSPF to use the specified value, instead of the actual interface MTU size.

Use the **no** variant of this command to return the MTU size to the default.

Syntax `ip ospf mtu <mtu-size>`
`no ip ospf mtu`

Parameter	Description
<mtu-size>	<576-65535> The MTU size in bytes.

Default OSPF uses the interface MTU derived from the interface

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command allows an administrator to configure the MTU size recognized by the OSPF protocol. It does not configure the MTU settings on the interface.

This command can be useful to ensure the OSPF neighbor relationship can fully establish via a network link, where the neighboring devices may have mismatched interface MTUs.

Example To change the OSPF MTU to 1446 on the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf mtu 1446
```

ip ospf mtu-ignore

Overview Use this command to configure OSPF so that OSPF does not check the MTU size during DD (Database Description) exchange.

Use the **no** variant of this command to make sure that OSPF checks the MTU size during DD exchange.

Syntax `ip ospf [<ip-address>] mtu-ignore`
`no ip ospf [<ip-address>] mtu-ignore`

Parameter	Description
<ip-address>	The IPv4 address of the interface, in dotted decimal notation.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes By default, during the DD exchange process, OSPF checks the MTU size described in the DD packets received from the neighbor. If the MTU size does not match the interface MTU, the neighbor adjacency is not established. Using this command makes OSPF ignore this check and allows establishing of adjacency regardless of MTU size in the DD packet.

Example To stop OSPF from checking the MTU size during DD exchange on the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf mtu-ignore
```

ip ospf network

Overview This command configures the OSPF network type to a type different from the default for the particular interface.

The **no** variant of this command returns the network type to the default for the particular interface.

Syntax `ip ospf network {broadcast|non-broadcast|point-to-point|point-to-multipoint}`
`no ip ospf network`

Parameter	Description
broadcast	Sets the network type to broadcast.
non-broadcast	Sets the network type to NBMA.
point-to-multipoint	Sets the network type to point-to-multipoint.
point-to-point	Sets the network type to point-to-point.

Default The default is the default type for the interface, e.g broadcast for eth interfaces.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command forces the interface network type to be the specified type. Depending on the network type, OSPF changes the behavior of the packet transmission and the link description in LSAs.

Example The following example shows setting the network type to point-to-point on the interface eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip ospf network point-to-point
```

ip ospf priority

Overview This command sets the router priority, which is a parameter used in the election of the designated router for the network.

The **no** variant of this command returns the router priority to the default of 1.

Syntax `ip ospf [<ip-address>] priority <priority>`
`no ip ospf [<ip-address>] priority`

Parameter	Description
<ip-address>	The IP address of the interface.
<priority>	<0-255> The Router Priority of the interface.

Default 1

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes Set the priority to help determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, the router with the higher router ID takes precedence.

Only routers with nonzero router priority values are eligible to become the designated or backup designated router.

Configure router priority for multi-access networks only and not for point-to-point networks.

Example To set the OSPF priority value to 3 on the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf priority 3
```

Related commands [ip ospf network](#)

ip ospf resync-timeout

Overview Use this command to set the interval after which adjacency is reset if out-of-band resynchronization has not occurred. The interval period starts from the time a restart signal is received from a neighbor.

Use the **no** variant of this command to return to the default.

Syntax `ip ospf [<ip-address>] resync-timeout <1-65535>`
`no ip ospf [<ip-address>] resync-timeout`

Parameter	Description
<ip-address>	The IP address of the interface.
<1-65535>	The resynchronization timeout value of the interface in seconds.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Example To set the OSPF resynchronization timeout value to 65 seconds on the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf resync-timeout 65
```

ip ospf retransmit-interval

Overview Use this command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

Use the **no** variant of this command to return to the default of 5 seconds.

Syntax `ip ospf [<ip-address>] retransmit-interval <1-65535>`
`no ip ospf [<ip-address>] retransmit-interval`

Parameter	Description
<ip-address>	The IP address of the interface.
<1-65535>	The interval in seconds.

Default 5 seconds

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgment. In case the router does not receive an acknowledgment during the set time (the retransmit interval value) it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.

Example To set the retransmit interval to 6 seconds on the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf retransmit-interval 6
```

ip ospf transmit-delay

Overview Use this command to set the estimated time it takes to transmit a link-state-update packet on the interface.

Use the **no** variant of this command to return to the default of 1 second.

Syntax `ip ospf [<ip-address>] transmit-delay <1-65535>`
`no ip ospf [<ip-address>] transmit-delay`

Parameter	Description
<ip-address>	The IP address of the interface.
<1-65535>	The time, in seconds, to transmit a link-state update.

Default 1 second

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Add transmission and propagation delays when setting the transmit delay value.

Example To set the OSPF transmit delay time to 3 seconds on the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip ospf transmit-delay 3
```

max-concurrent-dd

Overview Use this command to set the limit for the number of Database Descriptors (DD) that can be processed concurrently.

Use the **no** variant of this command to reset the limit for the number of Database Descriptors (DD) that can be processed concurrently.

Syntax `max-concurrent-dd <1-65535>`
`no max-concurrent-dd`

Parameter	Description
<code><1-65535></code>	Specify the number of DD processes.

Mode Router Configuration

Usage This command is useful when a router's performance is affected from simultaneously bringing up several OSPF adjacencies. This command limits the maximum number of DD exchanges that can occur concurrently per OSPF instance, thus allowing for all of the adjacencies to come up.

Example The following example sets the max-concurrent-dd value to 4, so that only 4 DD exchanges will be processed at a time.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# max-concurrent-dd 4
```

maximum-area

Overview Use this command to set the maximum number of OSPF areas.

Use the **no** variant of this command to set the maximum number of OSPF areas to the default.

Syntax `maximum-area <1-4294967294>`
`no maximum-area`

Parameter	Description
<code><1-4294967294></code>	Specify the maximum number of OSPF areas.

Default The default for the maximum number of OSPF areas is 4294967294.

Mode Router Configuration

Usage notes Use this command in router OSPF mode to specify the maximum number of OSPF areas.

Examples The following example sets the maximum number of OSPF areas to 2:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# maximum-area 2
```

The following example removes the maximum number of OSPF areas and resets to default:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# no maximum-area
```

neighbor (OSPF)

Overview Use this command to inform the router of other neighboring routers that are connected to the same Non-Broadcast Multiple Access (NBMA) network.

Use the **no** variant of this command to remove a configuration.

Syntax `neighbor <ip-address> [<cost>] {<priority>|<poll-interval>}`
`no neighbor <ip-address> [<cost>] {<priority>|<poll-interval>}`

Parameter	Description
<code><ip-address></code>	Specifies the interface IP address of the neighbor.
<code><priority></code>	<i>priority <0-255></i> Specifies the router priority value of the non-broadcast neighbor associated with the specified IP address. The default is 0. This keyword does not apply to point-to-multipoint interfaces.
<code><poll-interval></code>	<i>poll-interval <1-2147483647></i> Dead neighbor polling interval in seconds. It is recommended to set this value much higher than the hello interval. The default is 120 seconds.
<code><cost></code>	<i>cost <1-65535></i> Specifies the link-state metric to this neighbor.

Mode Router Configuration

Usage To configure a neighbor on an NBMA network manually, use the **neighbor** command and include one neighbor entry for each known non broadcast network neighbor. The IP address used in this command is the neighbor's primary IP address on the interface where that neighbor connects to the NBMA network.

The poll interval is the reduced rate at which routers continue to send hello packets, when a neighboring router has become inactive. Set the poll interval to be much larger than hello interval.

Examples This example shows a neighbor configured with a priority value, poll interval time, and cost:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# neighbor 1.2.3.4 priority 1
poll-interval 90
awplus(config-router)# neighbor 1.2.3.4 cost 15
```

network area

Overview Use this command to enable OSPF routing with a specified Area ID on any interfaces with IP addresses that match the specified network address.

Use the **no** variant of this command to disable OSPF routing on the interfaces.

Syntax `network <network-address> area <area-id>`
`no network <network-address> area <area-id>`

Parameter	Description
<code><network-address></code>	<code>{<ip-network/m> <ip-addr> <reverse-mask>}</code>
<code><ip-network/m></code>	IP address of the network, entered in the form A.B.C.D/M. Dotted decimal notation followed by a forward slash, and then the subnet mask length.
<code><ip-addr></code> <code><reverse-mask></code>	IPv4 network address, entered in the form A.B.C.D, followed by the mask. Enter the mask as a wildcard, or reverse, mask (e.g. 0.0.0.255). Note that the device displays the mask as a subnet mask in the running configuration.
<code><area-id></code>	<code>{<ip-addr> <0-4294967295>}</code>
<code><ip-addr></code>	OSPF Area ID in IPv4 address format, in the form A.B.C.D.
<code><0-4294967295></code>	OSPF Area ID as 4 octets unsigned integer value.

Default No **network area** is configured by default.

Mode Router Configuration

Usage notes OSPF routing can be enabled per IPv4 subnet. The network address can be defined using either the prefix length or a wild card mask. A wild card mask is comprised of consecutive 0's as network bits and consecutive 1's as host bits.

Examples The following commands show the use of the **network area** command with OSPF multiple instance support disabled:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# network 10.0.0.0/8 area 3
awplus(config-router)# network 10.0.0.0/8 area 1.1.1.1
```

The following commands disable OSPF routing with Area ID 3 on all interfaces:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# no network 10.0.0.0/8 area3
```


ospf abr-type

Overview Use this command to set an OSPF Area Border Router (ABR) type.
Use the **no** variant of this command to revert the ABR type to the default setting.

Syntax `ospf abr-type {cisco|ibm|standard}`
`no ospf abr-type [cisco|ibm|standard]`

Parameter	Description
cisco	Specifies an alternative ABR using Cisco implementation (RFC 3509). This is the default ABR type.
ibm	Specifies an alternative ABR using IBM implementation (RFC 3509).
standard	Specifies a standard behavior ABR (RFC 2328).

Default ABR type cisco

Mode Router Configuration

Usage Specifying the ABR type allows better interoperability between different implementations. This command is specially useful in a multi-vendor environment. The different ABR types are:

- Cisco ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case the configured backbone need not be actively connected.
- Standard ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached to it.

Example To configure the ABR type as **ibm**, use the following commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# ospf abr-type ibm
```

ospf restart grace-period

Overview Use this command to configure the grace-period for restarting OSPF routing.
Use the **no** variant of this command to revert to the default grace-period.

Syntax `ospf restart grace-period <1-1800>`
`no ospf restart grace-period`

Parameter	Description
<1-1800>	Specifies the grace period in seconds.

Default In the AlliedWare Plus™ OSPF implementation, the default OSPF grace-period is 180 seconds.

Mode Global Configuration

Usage notes Use this command to enable the OSPF Graceful Restart feature and set the restart grace-period. Changes from the default restart grace-period are displayed in the running- config. The restart grace-period is not displayed in the running-config if it has been reset to the default using the **no** variant of this command.

Example To set the OSPF restart grace-period to 250 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ospf restart grace-period 250
```

To reset the OSPF restart grace-period to the default (180 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# no ospf restart grace-period
```

Validation Commands [show running-config](#)

Related commands [ospf restart helper](#)
[restart ospf graceful](#)

ospf restart helper

Overview Use this command to configure the **helper** behavior for the OSPF Graceful Restart feature.

Use the **no** variant of this command to revert to the default grace-period.

Syntax

```
ospf restart helper {max-grace-period  
<grace-period>|only-reload|only-upgrade}  
ospf restart helper {never router-id <router-id>}  
no ospf restart helper [max-grace-period]
```

Parameter	Description
max-grace-period	Specify help if received grace-period is less than a specified value.
<grace-period>	Maximum grace period accepted in seconds in range <1-1800>.
never	Specify the local policy to never to act as a helper for this feature.
only-reload	Specify help only on software reloads not software upgrades.
only-upgrade	Specify help only on software upgrades not software reloads.
router-id	Enter the router-id keyword to specify the OSPF Router ID that is never to act as a helper for the OSPF Graceful Restart feature.
<router-id>	<A.B.C.D> Specify the OSPF Router ID in dotted decimal format A.B.C.D

Default In the AlliedWare Plus™ OSPF implementation, the default OSPF grace-period is 180 seconds.

Mode Global Configuration

Usage The **ospf restart helper** command requires at least one parameter, but you may use more than one in the same command (excluding parameter **never**).

The **no** version of this command turns off the OSPF restart helper, while the **no ospf restart helper max-grace-period** command resets the max-grace-period, rather than the helper policy itself.

Example

```
awplus# configure terminal  
awplus(config)# ospf restart helper only-reload  
awplus# configure terminal  
awplus(config)# ospf restart helper never router-id 10.10.10.1  
awplus# configure terminal  
awplus(config)# no ospf restart helper max-grace-period
```

**Related
commands** ospf restart grace-period
 restart ospf graceful

ospf router-id

Overview Use this command to specify a router ID for the OSPF process.
Use the **no** variant of this command to disable this function.

Syntax `ospf router-id <ip-address>`
`no ospf router-id`

Parameter	Description
<code><ip-address></code>	Specifies the router ID in IPv4 address format.

Mode Router Configuration

Usage Configure each router with a unique router-id. In an OSPF router process that has active neighbors, a new router-id takes effect at the next reload or when you restart OSPF manually.

Example The following example shows a specified router ID 2.3.4.5.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# ospf router-id 2.3.4.5
```

Related commands [show ip ospf](#)

overflow database

Overview Use this command to limit the maximum number of Link State Advertisements (LSAs) that can be supported by the current OSPF instance.

Use the **no** variant of this command to have no limit on the maximum number of LSAs.

Syntax `overflow database <0-4294967294> {hard|soft}`
`no overflow database`

Parameter	Description
<0-4294967294>	The maximum number of LSAs.
hard	Shutdown occurs if the number of LSAs exceeds the specified value.
soft	Warning message appears if the number of LSAs exceeds the specified value.

Mode Router Configuration

Usage Use **hard** with this command if a shutdown is required if the number of LSAs exceeds the specified number. Use **soft** with this command if a shutdown is not required, but a warning message is required, if the number of LSAs exceeds the specified number.

Example The following example shows setting the database overflow to 500, and a shutdown to occur, if the number of LSAs exceeds 500.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# overflow database 500 hard
```

overflow database external

Overview Use this command to configure the size of the external database and the time the router waits before it tries to exit the overflow state.

Use the **no** variant of this command to revert to default.

Syntax `overflow database external <max-lsas> <recover-time>`
`no overflow database external`

Parameter	Description
<code><max-lsas></code>	<code><0-2147483647></code> The maximum number of Link State Advertisements (LSAs). Note that this value should be the same on all routers in the AS.
<code><recover-time></code>	<code><0-65535></code> the number of seconds the router waits before trying to exit the database overflow state. If this parameter is 0, router exits the overflow state only after an explicit administrator command.

Mode Router Configuration

Usage Use this command to limit the number of AS-external-LSAs a router can receive, once it is in the wait state. It takes the number of seconds specified as the `<recover-time>` to recover from this state.

Example The following example shows setting the maximum number of LSAs to 5 and the time to recover from overflow state to be 3:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# overflow database external 50 3
```

passive-interface (OSPF)

Overview Use this command to suppress the sending of Hello packets on all interfaces, or on a specified interface. If you use the **passive-interface** command without the optional parameters then all interfaces are put into passive mode.

Use the **no** variant of this command to allow the sending of Hello packets on all interfaces, or on the specified interface. If you use the **no** variant of this command without the optional parameters then all interfaces are removed from passive mode.

Syntax `passive-interface [<interface>] [<ip-address>]`
`no passive-interface [<interface>] [<ip-address>]`

Parameter	Description
<interface>	The name of the interface.
<ip-address>	IP address of the interface, entered in the form A.B.C.D.

Mode Router Configuration

Usage notes Configure an interface to be passive if you wish its connected route to be treated as an OSPF route (rather than an AS-external route), but do not wish to actually exchange any OSPF packets via this interface.

Examples To configure passive interface mode on all interfaces, enter the following commands:

```
awplus(config)# router ospf 100
awplus(config-router)# passive-interface
```

To configure passive interface mode on the local loopback interface, enter the following commands:

```
awplus(config)# router ospf 100
awplus(config-router)# passive-interface lo
```

To remove passive interface mode on all interfaces, enter the following commands:

```
awplus(config)# router ospf 100
awplus(config-router)# no passive-interface
```


redistribute (OSPF)

Overview Use this command to redistribute routes from other routing protocols, static routes and connected routes into an OSPF routing table.

Use the **no** variant of this command to disable this function.

Syntax

```
redistribute {bgp|connected|rip|static} {metric  
<0-16777214>|metric-type {1|2}|route-map <name>|tag  
<0-4294967295>}  
  
no redistribute {bgp|connected|rip|static} {metric  
<0-16777214>|metric-type {1|2}|route-map <name>|tag  
<0-4294967295>}
```

Parameter	Description
bgp	Specifies that this applies to the redistribution of BGP routes.
connected	Specifies that this applies to the redistribution of connected routes.
rip	Specifies that this applies to the redistribution of RIP routes.
static	Specifies that this applies to the redistribution of static routes.
metric	Specifies the external metric.
metric-type	Specifies the external metric-type.
route-map	Specifies name of the route-map.
tag	Specifies the external route tag.

Default The default metric value for routes redistributed into OSPF is 20. The metric can also be defined using the [set metric](#) command for a route map. Note that a metric defined using the [set metric](#) command for a route map overrides a metric defined with this command.

Mode Router Configuration

Usage notes You use this command to inject routes, learned from other routing protocols, into the OSPF domain to generate AS-external-LSAs. If a route-map is configured by this command, then that route-map is used to control which routes are redistributed and can set metric and tag values on particular routes.

The metric, metric-type, and tag values specified on this command are applied to any redistributed routes that are not explicitly given a different metric, metric-type, or tag value by the route map.

See the [OSPF Feature Overview and Configuration Guide](#) for more information about metrics, and about behavior when configured in route maps.

Note that this command does not redistribute the default route. To redistribute the default route, use the [default-information originate](#) command.

Example The following example shows redistribution of BGP routes into OSPF routing table 100, with metric 12.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# redistribute bgp metric 12
```

The following example shows the configuration of a route-map named 'rmap2', which is then applied using the **redistribute route-map** command, so routes learned via a specified interface can be redistributed as type-1 external LSAs:

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 3
awplus(config-route-map)# match interface eth1
awplus(config-route-map)# set metric-type 1
awplus(config-route-map)# exit
awplus(config)# router ospf 100
awplus(config-router)# redistribute rip route-map rmap2
```

Note that configuring a route-map and applying it with the **redistribute route-map** command allows you to filter which routes are distributed from another routing protocol (such as RIP). A route-map can also set the metric, tag, and metric-type of the redistributed routes.

Related commands [match interface](#)
[route-map](#)

[show ip ospf database external](#)

restart ospf graceful

Overview Use this command to force the OSPF process to restart, and optionally set the grace-period.

Syntax `restart ospf graceful [grace-period <1-1800>]`

Parameter	Description
grace-period	Specify the grace period.
<1-1800>	The grace period in seconds.

Default In the AlliedWare Plus™ OSPF implementation, the default OSPF grace-period is 180 seconds.

Mode Privileged Exec

Usage notes After this command is executed, the OSPF process immediately shuts down. It notifies the system that OSPF has performed a graceful shutdown. Routes installed by OSPF are preserved until the grace-period expires.

When a **restart ospf graceful** command is issued, the OSPF configuration is reloaded from the last saved configuration. Ensure you first enter the command [copy running-config startup-config](#).

Example

```
awplus# copy running-config startup-config
awplus# restart ospf graceful grace-period 200
```

Related commands [ospf restart grace-period](#)
[ospf restart helper](#)

router ospf

Overview Use this command to enter Router Configuration mode to configure an OSPF routing process. You must specify the process ID with this command for multiple OSPF routing processes on the device.

Use the **no** variant of this command to terminate an OSPF routing process.

Use the **no** parameter with the **process-id** parameter, to terminate and delete a specific OSPF routing process. If no **process-id** is specified on the **no** variant of this command, then all OSPF routing processes are terminated, and all OSPF configuration is removed.

Syntax `router ospf [<process-id>]`
`no router ospf [<process-id>]`

Parameter	Description
<process-id>	A positive number from 1 to 65535, that is used to define a routing process.

Default No routing process is defined by default.

Mode Global Configuration

Usage notes The process ID of OSPF is an optional parameter for the **no** variant of this command only. When removing all instances of OSPF, you do not need to specify each Process ID, but when removing particular instances of OSPF you must specify each Process ID to be removed.

Example To enter Router Configuration mode to configure an existing OSPF routing process 100, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)#
```

Command changes Version 5.4.6-2.1: VRF-lite support added.

router-id

Overview Use this command to specify a router ID for the OSPF process.

Use the **no** variant of this command to force OSPF to use the previous OSPF router-id behavior.

Syntax `router-id <ip-address>`
`no router-id`

Parameter	Description
<code><ip-address></code>	Specifies the router ID in IPv4 address format.

Mode Router Configuration

Usage Configure each router with a unique router-id. In an OSPF router process that has active neighbors, a new router-id is used at the next reload or when you restart OSPF manually.

Example The following example shows a fixed router ID 10.10.10.60

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# router-id 10.10.10.60
```

Related commands [show ip ospf](#)

show debugging ospf

Overview Use this command to see what debugging is turned on for OSPF.
For information on filtering and saving command output, see the [“Getting_Started with AlliedWare Plus” Feature Overview and Configuration_Guide](#).

Syntax `show debugging ospf`

Mode User Exec and Privileged Exec

Example `awplus# show debugging ospf`

Output Figure 22-2: Example output from the **show debugging ospf** command

```
OSPF debugging status:
  OSPF packet Link State Update debugging is on
  OSPF all events debugging is on
```

show ip ospf

Overview Use this command to display general information about all OSPF routing processes. Include the process ID parameter with this command to display information about specified instances.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf`
`show ip ospf <process-id>`

Parameter	Description
<process-id>	<0-65535> The ID of the router process for which information will be displayed. If this parameter is included, only the information for the specified routing process is displayed.

Mode User Exec and Privileged Exec

Examples To display general information about all OSPF routing processes, use the command:

```
awplus# show ip ospf
```

To display general information about OSPF routing process 100, use the command:

```
awplus# show ip ospf 100
```

Table 1: Example output from the **show ip ospf** command

```
Route Licence: Route : Limit=0, Allocated=0, Visible=0, Internal=0
Route Licence: Breach: Current=0, Watermark=0
Routing Process "ospf 10" with ID 192.168.1.1
Process uptime is 10 hours 24 minutes
Process bound to VRF default
Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
Supports Graceful Restart
SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0 secs
Refresh timer 10 secs
Number of incoming current DD exchange neighbors 0/5
Number of outgoing current DD exchange neighbors 0/5
Number of external LSA 0. Checksum 0x000000
Number of opaque AS LSA 0. Checksum 0x000000
Number of non-default external LSA 0
```

Table 1: Example output from the **show ip ospf** command (cont.)

```
External LSA database is unlimited.
Number of LSA originated 0
Number of LSA received 0
Number of areas attached to this router: 2
  Area 0 (BACKBONE) (Inactive)
    Number of interfaces in this area is 0(0)
    Number of fully adjacent neighbors in this area is 0
    Area has no authentication
    SPF algorithm executed 0 times
    Number of LSA 0. Checksum 0x000000

  Area 1 (Inactive)
    Number of interfaces in this area is 0(0)
    Number of fully adjacent neighbors in this area is 0
    Number of fully adjacent virtual neighbors through this area is 0
    Area has no authentication
    SPF algorithm executed 0 times
    Number of LSA 0. Checksum 0x000000
```

Table 2: Example output from the **show ip ospf <process-id>** command

```
Routing Process "ospf 100" with ID 10.10.11.146
Process uptime is 0 minute
Conforms to RFC2328, and RFC1583Compatibility flag is disabled
Supports only single TOS(TOS0) routes
Supports opaque LSA
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Refresh timer 10 secs
Number of external LSA 0. Checksum Sum 0x0
Number of non-default external LSA 0
External LSA database is unlimited.
Number of areas attached to this router: 1
  Area 1
    Number of interfaces in this area is 1(1)
    Number of fully adjacent neighbors in this area is 0
    Number of fully adjacent virtual neighbors through this area is 0
    Area has no authentication
    SPF algorithm executed 0 times
    Number of LSA 1. Checksum Sum 0x00e3e2
```


Table 3: Parameters in the output of the **show ip ospf** command

Output Parameter		Meaning
Route Licence: Route:	Limit	The maximum number of OSPF routes which may be used for forwarding.
	Allocated	The current total number of OSPF routes allocated in the OSPF module.
	Visible	The current number of OSPF routes which may be used for forwarding.
	Internal	The number of OSPF internal routes used for calculating paths to ASBRs.
Number of external LSA		The number of external link-state advertisements
Number of opaque AS LSA		Number of opaque link-state advertisements

Related commands [router ospf](#)

show ip ospf border-routers

Overview Use this command to display the ABRs and ASBRs for all OSPF instances. Include the process ID parameter with this command to view data about specified instances.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf border-routers`
`show ip ospf <process-id> border-routers`

Parameter	Description
<process-id>	<0-65535> The ID of the router process for which information will be displayed.

Mode User Exec and Privileged Exec

Examples To display the ABRs and ASBRs for all OSPF instances, use the following command:

```
awplus# show ip ospf border-routers
```

Output Figure 22-3: Example output from the **show ip ospf border-routers** command

```
OSPF process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.15.0.1 [10] via 10.10.0.1, eth1, ASBR, Area 0.0.0.0
...
```

show ip ospf database

Overview Use this command to display a database summary for OSPF information. Include the process ID parameter with this command to display information about specified instances.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf [<process-id>] database`
`[self-originate|max-age|adv router <adv-router-id>]`

Parameter	Description
<process-id>	<0-65535> The ID of the router process for which information will be displayed.
self-originate	Displays self-originated link states.
max-age	Displays LSAs in MaxAge list. It maintains the list of the all LSAs in the database which have reached the max-age which is 3600 seconds.
adv-router	Advertising Router LSA.
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.

Mode User Exec and Privileged Exec

Examples To display the ABRs and ASBRs for all OSPF instances, use the command:

```
awplus# show ip ospf border-routers
```

To display the ABRs and ASBRs for the specific OSPF instance 721, use the command:

```
awplus# show ip ospf 721 border-routers
```

Output Figure 22-4: Example output from the **show ip ospf database** command

OSPF Router process 1 with ID (10.10.11.60)					
Router Link States (Area 0.0.0.1)					
Link ID	ADV Router	Age	Seq#	CkSum	Link
count					
10.10.11.60	10.10.11.60	32	0x80000002	0x472b	1
OSPF Router process 100 with ID (10.10.11.60)					
Router Link States (Area 0.0.0.0)					
Link ID	ADV Router	Age	Seq#	CkSum	Link
count					
10.10.11.60	10.10.11.60	219	0x80000001	0x4f5d	0

Example awplus# show ip ospf database external 1.2.3.4 self-originate
awplus# show ip ospf database self-originate

Figure 22-5: Example output from the **show ip ospf database self-originate** command

OSPF Router process 100 with ID (10.10.11.50)					
Router Link States (Area 0.0.0.1 [NSSA])					
Link ID	ADV Router	Age	Seq#	CkSum	Link
count					
10.10.11.50	10.10.11.50	20	0x80000007	0x65c3	2
Area-Local Opaque-LSA (Area 0.0.0.1 [NSSA])					
Link ID	ADV Router	Age	Seq#	CkSum	Opaque ID
67.1.4.217	10.10.11.50	37	0x80000001	0x2129	66777
AS-Global Opaque-LSA					
Link ID	ADV Router	Age	Seq#	CkSum	Opaque ID
67.1.4.217	10.10.11.50	37	0x80000001	0x2daa	66777

show ip ospf database asbr-summary

Overview Use this command to display information about the Autonomous System Boundary Router (ASBR) summary LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus”_Feature Overview and Configuration Guide](#).

Syntax `show ip ospf database asbr-summary [<ip-addr>]
[self-originate|adv-router <advrouter-ip-addr>]`

Parameter	Description
<ip-addr>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.
adv-router <advrouter-ip-addr>	Displays all the LSAs of the specified router.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database asbr-summary 1.2.3.4  
self-originate  
  
awplus# show ip ospf database asbr-summary self-originate  
  
awplus# show ip ospf database asbr-summary 1.2.3.4 adv-router  
2.3.4.5
```

show ip ospf database external

Overview Use this command to display information about the external LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf database external adv-router[<adv-router-id>]
[self-originate|adv-router<adv-router-id>]`

Parameter	Description
adv-router	Displays all the LSAs of the specified router.
self-originate	Displays self-originated link states.
<adv-router- id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.

Mode User Exec and Privileged Exec

Examples `awplus# show ip ospf database external 1.2.3.4 self-originate`
`awplus# show ip ospf database external self-originate`
`awplus# show ip ospf database external 1.2.3.4 adv-router 2.3.4.5`

Output Figure 22-6: Example output from the **show ip ospf database external self-originate** command

```
OSPF Router process 100 with ID (10.10.11.50)
  AS External Link States
LS age: 298
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 10.10.100.0 (External Network Number)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x7033
Length: 36
Network Mask: /24
  Metric Type: 2 (Larger than any link state path)
  TOS: 0
  Metric: 20
  Forward Address: 10.10.11.50
  External Route Tag: 0
```

Output Figure 22-7: Example output from the **show ip ospf database external adv-router** command

```
awplus#show ip ospf database external adv-router 1.1.1.1

                        AS External Link States
LS age: 273
Options: 0x2 (-|-|-|-|-|E|-)
LS Type: AS-external-LSA
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 1.1.1.1
LS Seq Number: 80000004
Checksum: 0x02f8
Length: 36
Network Mask: /24
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 20
    Forward Address: 0.0.0.0
    External Route Tag: 0
```

show ip ospf database network

Overview Use this command to display information about the network LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf database network [<adv-router-id>]
[self-originate|<adv-router-id>]`

Parameter	Description
<adv-router-id>	The router ID of the advertising router, in IPv4 address format. Note however, that this no longer represents a real address.
self-originate	Displays self-originated link states.
adv-router	Displays all the LSAs of the specified router.

Mode User Exec and Privileged Exec

Examples `awplus# show ip ospf database network 1.2.3.4 self-originate`
`awplus# show ip ospf database network self-originate`
`awplus# show ip ospf database network 1.2.3.4 adv-router 2.3.4.5`

Output Figure 22-8: Example output from the **show ip ospf database network** command

```
OSPF Router process 200 with ID (192.30.30.2)
  Net Link States (Area 0.0.0.0)
LS age: 1387
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: network-LSA
Link State ID: 192.10.10.9 (address of Designated Router)
Advertising Router: 192.30.30.3
LS Seq Number: 80000001
Checksum: 0xelb0
Length: 32
Network Mask: /24
  Attached Router: 192.20.20.1
  Attached Router: 192.30.30.3
OSPF Router process 200 with ID (192.30.30.2)
  Net Link States (Area 0.0.0.0)
...
```


show ip ospf database nssa-external

Overview Use this command to display information about the NSSA external LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf database nssa-external [<ip-address>]
[self-originate|<advrouter>]`

Parameter	Description
<advrouter>	adv-router <ip-address>
adv-router	Displays all the LSAs of the specified router.
<ip-address>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.

Mode User Exec and Privileged Exec

Examples `awplus# show ip ospf database nssa-external 1.2.3.4
self-originate`

`awplus# show ip ospf database nssa-external self-originate`

`awplus# show ip ospf database nssa-external 1.2.3.4 adv-router
2.3.4.5`

Output Figure 22-9: Example output from the **show ip ospf database nssa-external adv-router** command

```
OSPF Router process 100 with ID (10.10.11.50)
  NSSA-external Link States (Area 0.0.0.0)
  NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 78
Options: 0x0 (*|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 0.0.0.0 (External Network Number For NSSA)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0xc9b6
Length: 36
Network Mask: /0
  Metric Type: 2 (Larger than any link state path)
  TOS: 0
  Metric: 1
  NSSA: Forward Address: 0.0.0.0
```

```
      OSPF Router process 100 with ID (10.10.11.50)
        NSSA-external Link States (Area 0.0.0.0)
        NSSA-external Link States (Area 0.0.0.1 [NSSA])
LS age: 78
Options: 0x0 (*|-|-|-|-|-|-)
LS Type: AS-NSSA-LSA
Link State ID: 0.0.0.0 (External Network Number For NSSA)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0xc9b6
Length: 36
Network Mask: /0
    Metric Type: 2 (Larger than any link state path)
    TOS: 0
    Metric: 1
    NSSA: Forward Address: 0.0.0.0
    External Route Tag: 0
        NSSA-external Link States (Area 0.0.0.1 [NSSA])
```

show ip ospf database opaque-area

Overview Use this command to display information about the area-local (link state type 10) scope LSAs. Type-10 Opaque LSAs are not flooded beyond the borders of their associated area.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf database opaque-area [<ip-address>]
[self-originate|<advrouter>]`

Parameter	Description
<advrouter>	adv-router <ip-address>
adv-router	Displays all the LSAs of the specified router.
<ip-address>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database opaque-area 1.2.3.4  
self-originate  
  
awplus# show ip ospf database opaque-area self-originate  
  
awplus# show ip ospf database opaque-area 1.2.3.4 adv-router  
2.3.4.5
```

Output Figure 22-10: Example output from the **show ip ospf database opaque-area** command

```
OSPF Router process 100 with ID (10.10.11.50)
      Area-Local Opaque-LSA (Area 0.0.0.0)
LS age: 262
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: Area-Local Opaque-LSA
Link State ID: 10.0.25.176 (Area-Local Opaque-Type/ID)
Opaque Type: 10
Opaque ID: 6576
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0xb413
Length: 26
```

show ip ospf database opaque-as

Overview Use this command to display information about the link-state type 11 LSAs. This type of link-state denotes that the LSA is flooded throughout the Autonomous System (AS).

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf database opaque-as [<ip-address>]
[self-originate|<advrouter>]`

Parameter	Description
<advrouter>	adv-router <ip-address>
adv-router	Displays all the LSAs of the specified router.
<ip-address>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.

Mode User Exec and Privileged Exec

Examples `awplus# show ip ospf database opaque-as 1.2.3.4 self-originate`
`awplus# show ip ospf database opaque-as self-originate`
`awplus# show ip ospf database opaque-as 1.2.3.4 adv-router`
`2.3.4.5`

Output Figure 22-11: Example output from the **show ip ospf database opaque-as** command

```
OSPF Router process 100 with ID (10.10.11.50)
AS-Global Opaque-LSA
LS age: 325
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: AS-external Opaque-LSA
Link State ID: 11.10.9.23 (AS-external Opaque-Type/ID)
Opaque Type: 11
Opaque ID: 657687
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0xb018
Length: 25
```

show ip ospf database opaque-link

Overview Use this command to display information about the link-state type 9 LSAs. This type denotes a link-local scope. The LSAs are not flooded beyond the local network.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf database opaque-link [<ip-address>]
[self-originate|<advrouter>]`

Parameter	Description
<advrouter>	adv-router <ip-address>
adv-router	Displays all the LSAs of the specified router.
<ip-address>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip ospf database opaque-link 1.2.3.4  
self-originate  
  
awplus# show ip ospf database opaque-link self-originate  
  
awplus# show ip ospf database opaque-link 1.2.3.4 adv-router  
2.3.4.5
```

Output Figure 22-12: Example output from the **show ip ospf database opaque-link** command

```
OSPF Router process 100 with ID (10.10.11.50)
      Link-Local Opaque-LSA (Link hme0:10.10.10.50)
LS age: 276
Options: 0x2 (*|---|E|)
LS Type: Link-Local Opaque-LSA
Link State ID: 10.0.220.247 (Link-Local Opaque-Type/ID)
Opaque Type: 10
Opaque ID: 56567
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x744e
Length: 26
      Link-Local Opaque-LSA (Link hme1:10.10.11.50)
```

show ip ospf database router

Overview Use this command to display information only about the router LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf database router [<adv-router-id>
self-originate|<adv-router-id>]`

Parameter	Description
adv-router	Displays all the LSAs of the specified router.
self-originate	Displays self-originated link states.
<adv-router- id>	The router ID of the advertising router, in IPv4 address format. Note however, that this no longer represents a real address.

Mode User Exec and Privileged Exec

Examples `awplus# show ip ospf database router 1.2.3.4 self-originate`
`awplus# show ip ospf database router self-originate`
`awplus# show ip ospf database router 1.2.3.4 adv-router 2.3.4.5`

Output Figure 22-13: Example output from the **show ip ospf database router** command

```
OSPF Router process 100 with ID (10.10.11.50)
Router Link States (Area 0.0.0.0)

LS age: 878
Options: 0x2 (*|-|-|-|-|E|-)
Flags: 0x3 : ABR ASBR
LS Type: router-LSA
Link State ID: 10.10.11.50
Advertising Router: 10.10.11.50
LS Seq Number: 80000004
Checksum: 0xe39e
Length: 36
Number of Links: 1
  Link connected to: Stub Network
    (Link ID) Network/subnet number: 10.10.10.0
    (Link Data) Network Mask: 255.255.255.0
  Number of TOS metrics: 0
    TOS 0 Metric: 10
```

```
Router Link States (Area 0.0.0.1)
LS age: 877
Options: 0x2 (*|---|E|)
Flags: 0x3 : ABR ASBR
LS Type: router-LSA
Link State ID: 10.10.11.50
Advertising Router: 10.10.11.50
LS Seq Number: 80000003
Checksum: 0xee93
Length: 36
  Number of Links: 1
    Link connected to: Stub Network
      (Link ID) Network/subnet number: 10.10.11.0
      (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
        TOS 0 Metric: 10
```

show ip ospf database summary

Overview Use this command to display information about the summary LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf database summary [<ip-address>]
[self-originate|<advrouter>]`

Parameter	Description
<advrouter>	adv-router <ip-address>
adv-router	Displays all the LSAs of the specified router.
<ip-address>	A link state ID, as an IP address.
self-originate	Displays self-originated link states.

Mode User Exec and Privileged Exec

Examples `awplus# show ip ospf database summary 1.2.3.4 self-originate`
`awplus# show ip ospf database summary self-originate`
`awplus# show ip ospf database summary 1.2.3.4 adv-router 2.3.4.5`

Output Figure 22-14: Example output from the **show ip ospf database summary** command

```
OSPF Router process 100 with ID (10.10.11.50)
    Summary Link States (Area 0.0.0.0)
    Summary Link States (Area 0.0.0.1)
LS age: 1124
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: summary-LSA
Link State ID: 10.10.10.0 (summary Network Number)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x41a2
Length: 28
Network Mask: /24
    TOS: 0   Metric: 10
```


Figure 22-15: Example output from the **show ip ospf database summary self-originate** command

```
OSPF Router process 100 with ID (10.10.11.50)
  Summary Link States (Area 0.0.0.0)
    LS age: 1061
    Options: 0x2 (*|-|-|-|-|E|-)
    LS Type: summary-LSA
    Link State ID: 10.10.11.0 (summary Network Number)
    Advertising Router: 10.10.11.50
    LS Seq Number: 80000001
    Checksum: 0x36ac
    Length: 28
    Network Mask: /24
      TOS: 0  Metric: 10
  Summary Link States (Area 0.0.0.1)
    LS age: 1061
    Options: 0x2 (*|-|-|-|-|E|-)
    LS Type: summary-LSA
    Link State ID: 10.10.11.0 (summary Network Number)
    Advertising Router: 10.10.11.50
    LS Seq Number: 80000001
    Checksum: 0x36ac
    Length: 28
    Network Mask: /24
      TOS: 0  Metric: 10
  Summary Link States (Area 0.0.0.1)
    LS age: 1061
    Options: 0x2 (*|-|-|-|-|E|-)
    LS Type: summary-LSA
    Link State ID: 10.10.10.0 (summary Network Number)
    Advertising Router: 10.10.11.50
    LS Seq Number: 80000001
    Checksum: 0x41a2
    Length: 28
    Network Mask: /24
      TOS: 0  Metric: 10
```

Figure 22-16: Example output from the **show ip ospf database summary**
adv-router <ip-address> command

```
OSPF Router process 100 with ID (10.10.11.50)
  Summary Link States (Area 0.0.0.0)
LS age: 989
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: summary-LSA
Link State ID: 10.10.11.0 (summary Network Number)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x36ac
Length: 28
Network Mask: /24
      TOS: 0   Metric: 10
  Summary Link States (Area 0.0.0.1)
LS age: 989
Options: 0x2 (*|-|-|-|-|E|-)
LS Type: summary-LSA
Link State ID: 10.10.11.0 (summary Network Number)
Advertising Router: 10.10.11.50
LS Seq Number: 80000001
Checksum: 0x36ac
Length: 28
Network Mask: /24
      TOS: 0   Metric: 10
```

show ip ospf interface

Overview Use this command to display interface information for OSPF.

For information on filtering and saving command output, see the [“Getting_Started with AlliedWare Plus” Feature Overview and Configuration_Guide](#).

Syntax `show ip ospf interface [<interface-list>]`

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • a PPP interface (e.g. ppp0) • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the encapsulation dot1q command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • a tunnel interface (e.g. tunnel0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list.

Mode User Exec and Privileged Exec

Examples `awplus# show ip ospf interface tunnel14`

Output Figure 22-17: Example output from the **show ip ospf interface** command

```
awplus#show ip ospf interface
tunnel14 is up, line protocol is up
 Internet Address 192.168.100.5/30, Area 0.0.0.200, MTU 1438
 Interface state Point-To-Point
 Process ID 200, Router ID 10.255.255.1, Network Type POINTOPOINT, Cost: 1
 Transmit Delay is 1 sec, State Point-To-Point
 Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
   Hello due in 00:00:06
 Neighbor Count is 1, Adjacent neighbor count is 0
 Crypt Sequence Number is 237068
 Hello received 1211 sent 1259, DD received 9 sent 20
 LS-Req received 3 sent 2, LS-Upd received 19 sent 231
 LS-Ack received 218 sent 17, Discarded 0
```

show ip ospf neighbor

Overview Use this command to display information on OSPF neighbors. Include the **ospf-id** parameter with this command to display information about specified instances.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf [<ospf-id>] neighbor <neighbor-ip-addr> [detail]`
`show ip ospf [<ospf-id>] neighbor detail [all]`
`show ip ospf [<ospf-id>] neighbor [all]`
`show ip ospf [<ospf-id>] neighbor interface <ip-addr>`

Parameter	Description
<ospf-id>	<0-65535> The ID of the router process for which information will be displayed.
<neighbor-ip-addr>	The Neighbor ID, entered as an IP address.
all	Include downstatus neighbor.
detail	Detail of all neighbors.
<ip-addr>	IP address of the interface.

Mode User Exec and Privileged Exec

Examples `awplus# show ip ospf neighbor detail`
`awplus# show ip ospf neighbor 1.2.3.4`
`awplus# show ip ospf neighbor interface 10.10.10.50 detail all`

Output Note that before a device enters OSPF Graceful Restart it first informs its OSPF neighbors. In the **show** output, an * symbol beside the **Dead Time** parameter indicates that the device has been notified of a neighbor entering the graceful restart state.

Figure 22-18: Example output from the **show ip ospf neighbor** command

```
awplus#show ip ospf neighbor

OSPF process 200:
Neighbor ID    Pri   State           Dead Time   Address        Interface
192.168.100.22  1     Full/ -         00:00:32    192.168.100.18 tunnel16
...
```

Figure 22-19: Example output from the **show ip ospf <ospf-id> neighbor** command

```
awplus#show ip ospf 200 neighbor

OSPF process 200:
Neighbor ID      Pri   State           Dead Time   Address        Interface
192.168.100.22   1     Full/ -         00:00:32    192.168.100.18 tunnel16
```

Figure 22-20: Example output from the **show ip ospf neighbor detail** command

```
awplus#show ip ospf neighbor detail
Neighbor 192.168.100.22, interface address 192.168.100.18
  In the area 0.0.0.200 via interface tunnel16
  Neighbor priority is 1, State is Full, 5 state changes
  DR is 0.0.0.0, BDR is 0.0.0.0
  Options is 0x42 (-|O|-|-|-|E|-)
  Dead timer due in 00:00:34
  Neighbor is up for 02:08:06
  Database Summary List 0
  Link State Request List 0
  Link State Retransmission List 0
  Crypt Sequence Number is 0
  Thread Inactivity Timer on
  Thread Database Description Retransmission off
  Thread Link State Request Retransmission off
  Thread Link State Update Retransmission off
```

show ip ospf route

Overview Use this command to display the OSPF routing table. Include the **ospf-id** parameter with this command to display the OSPF routing table for specified instances.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf [<ospf-id>] route`

Parameter	Description
<ospf-id>	<0-65535> The ID of the router process for which information will be displayed. If this parameter is included, only the information for this specified routing process is displayed.

Mode User Exec and Privileged Exec

Examples To display the OSPF routing table, use the command:

```
awplus# show ip ospf route
```

Output Figure 22-21: Example output from the **show ip ospf route** command for a specific process

```
awplus#show ip ospf route

OSPF process 200:
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2

O 172.30.1.64/26 [2] via 192.168.100.6, tunnel104, Area 0.0.0.200
O 172.30.2.64/26 [2] via 192.168.100.18, tunnel116, Area 0.0.0.200
O 172.30.4.0/24 [2] via 192.168.100.6, tunnel104, Area 0.0.0.200
C 192.168.100.4/30 [1] is directly connected, tunnel104, Area 0.0.0.200
C 192.168.100.16/30 [1] is directly connected, tunnel116, Area 0.0.0.200
```

show ip ospf virtual-links

Overview Use this command to display virtual link information.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip ospf virtual-links`

Mode User Exec and Privileged Exec

Examples To display virtual link information, use the command:

```
awplus# show ip ospf virtual-links
```

Output Figure 22-22: Example output from the **show ip ospf virtual-links** command

```
awplus#show ip ospf virtual-links
Virtual Link VLINK0 to router 10.10.0.9 is up
  Transit area 0.0.0.1 via interface eth1
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in 00:00:02
    Adjacency state Full
Virtual Link VLINK1 to router 10.10.0.123 is down
  Transit area 0.0.0.1 via interface *
  Transmit Delay is 1 sec, State Down,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in inactive
    Adjacency state Down
```

show ip protocols ospf

Overview Use this command to display OSPF process parameters and statistics.
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ip protocols ospf`

Mode User Exec and Privileged Exec

Examples To display OSPF process parameters and statistics, use the command:

```
awplus# show ip protocols ospf
```

Output Figure 22-23: Example output from the **show ip protocols ospf** command

```
Routing Protocol is "ospf 200"
  Invalid after 0 seconds, hold down 0, flushed after 0
  Outgoing update filter list for all interfaces is
    Redistributed kernel filtered by filter1
  Incoming update filter list for all interfaces is
  Redistributing: kernel
  Routing for Networks:
    192.30.30.0/24
    192.40.40.0/24
  Routing Information Sources:
    Gateway          Distance          Last Update
  Distance: (default is 110)
    Address          Mask              Distance List
```


summary-address

Overview Use this command to summarize, or possibly suppress, external routes that have the specified address range.

Use the **no** variant of this command to stop summarizing, or suppressing, external routes that have the specified address range.

Syntax `summary-address <ip-addr/prefix-length> [not-advertise] [tag <0-4294967295>]`
`no summary-address <ip-addr/prefix-length> [not-advertise] [tag <0-4294967295>]`

Parameter	Description
<code><ip-addr/prefix-length></code>	Specifies the base IP address of the summary address. The range of addresses given as IPv4 starting address and a prefix length.
<code>not-advertise</code>	Set the not-advertise option if you do not want OSPF to advertise either the summary address or the individual networks within the range of the summary address.
<code>tag <0-4294967295></code>	The tag parameter specifies the tag value that OSPF places in the AS external LSAs created as a result of redistributing the summary route. The tag overrides tags set by the original route.

Default The default tag value for a summary address is 0.

Mode Router Configuration

Usage notes An address range is a pairing of an address and a mask that is almost the same as IP network number. For example, if the specified address range is 192.168.0.0/255.255.240.0, it matches: 192.168.1.0/24, 192.168.4.0/22, 192.168.8.128/25 and so on.

Redistributing routes from other protocols into OSPF requires the router to advertise each route individually in an external LSA. Use the **summary address** command to advertise one summary route for all redistributed routes covered by a specified network address and mask. This helps decrease the size of the OSPF link state database.

Ensure OSPF routes exist in the summary address range for advertisement before using this command.

Example The following example uses the **summary-address** command to aggregate external LSAs that match the network 172.16.0.0/16 and assign a Tag value of 3.

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# summary-address 172.16.0.0/16 tag 3
```

timers spf exp

Overview Use this command to adjust route calculation timers using exponential back-off delays.

Use **no** form of this command to return to the default exponential back-off timer values.

Syntax `timers spf exp <min-holdtime> <max-holdtime>`
`no timers spf exp`

Parameter	Description
<code><min-holdtime></code>	<code><0-2147483647></code> Specifies the minimum delay between receiving a change to the SPF calculation in milliseconds. The default SPF min-holdtime value is 50 milliseconds.
<code><max-holdtime></code>	<code><0-2147483647></code> Specifies the maximum delay between receiving a change to the SPF calculation in milliseconds. The default SPF max-holdtime value is 50 seconds.

Mode Router Configuration

Default The default SPF min-holdtime is 50 milliseconds. The default SPF max-holdtime is 40 seconds.

Usage This command configures the minimum and maximum delay time between the receipt of a topology change and the calculation of the Shortest Path First (SPF).

Examples To set the minimum delay time to 5 milliseconds and maximum delay time to 10 milliseconds, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# timers spf exp 5 10
```

To reset the minimum and maximum delay times to the default values, use the commands:

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# no timers spf exp
```

Related commands [timers spf exp](#)

undebbug ospf events

Overview This command applies the functionality of the no [debug ospf events](#) command.

undebbug ospf ifsm

Overview This command applies the functionality of the no `debug ospf ifsm` command.

undebg ospf lsa

Overview This command applies the functionality of the no [debug ospf lsa](#) command.

undebbug ospf nfsm

Overview This command applies the functionality of the no `debug ospf nfsm` command.

undebbug ospf nsm

Overview This command applies the functionality of the no `debug ospf nsm` command.

undebg ospf packet

Overview This command applies the functionality of the no `debug ospf packet` command.

undebbug ospf route

Overview This command applies the functionality of the no [debug ospf route](#) command.

23

OSPFv3 for IPv6 Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure OSPFv3 for IPv6. See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information and examples.

- Command List**
- [“abr-type”](#) on page 833
 - [“area authentication ipsec spi”](#) on page 834
 - [“area default-cost \(IPv6 OSPF\)”](#) on page 836
 - [“area encryption ipsec spi esp”](#) on page 837
 - [“area range \(IPv6 OSPF\)”](#) on page 840
 - [“area stub \(IPv6 OSPF\)”](#) on page 842
 - [“area virtual-link \(IPv6 OSPF\)”](#) on page 843
 - [“area virtual-link authentication ipsec spi”](#) on page 845
 - [“area virtual-link encryption ipsec spi”](#) on page 847
 - [“auto-cost reference bandwidth \(IPv6 OSPF\)”](#) on page 850
 - [“bandwidth”](#) on page 852
 - [“clear ipv6 ospf process”](#) on page 853
 - [“debug ipv6 ospf events”](#) on page 854
 - [“debug ipv6 ospf ifsm”](#) on page 855
 - [“debug ipv6 ospf lsa”](#) on page 856
 - [“debug ipv6 ospf nfsm”](#) on page 857
 - [“debug ipv6 ospf packet”](#) on page 858
 - [“debug ipv6 ospf route”](#) on page 859
 - [“default-information originate”](#) on page 860

- [“default-metric \(IPv6 OSPF\)”](#) on page 861
- [“distance \(IPv6 OSPF\)”](#) on page 862
- [“ipv6 ospf authentication spi”](#) on page 864
- [“ipv6 ospf cost”](#) on page 866
- [“ipv6 ospf dead-interval”](#) on page 867
- [“ipv6 ospf display route single-line”](#) on page 868
- [“ipv6 ospf encryption spi esp”](#) on page 869
- [“ipv6 ospf hello-interval”](#) on page 872
- [“ipv6 ospf neighbor”](#) on page 873
- [“ipv6 ospf network”](#) on page 875
- [“ipv6 ospf priority”](#) on page 876
- [“ipv6 ospf retransmit-interval”](#) on page 877
- [“ipv6 ospf transmit-delay”](#) on page 878
- [“ipv6 router ospf area”](#) on page 879
- [“max-concurrent-dd \(IPv6 OSPF\)”](#) on page 881
- [“passive-interface \(IPv6 OSPF\)”](#) on page 882
- [“redistribute \(IPv6 OSPF\)”](#) on page 883
- [“restart ipv6 ospf graceful”](#) on page 885
- [“router ipv6 ospf”](#) on page 886
- [“router-id \(IPv6 OSPF\)”](#) on page 887
- [“show debugging ipv6 ospf”](#) on page 888
- [“show ipv6 ospf”](#) on page 889
- [“show ipv6 ospf database”](#) on page 891
- [“show ipv6 ospf database external”](#) on page 892
- [“show ipv6 ospf database grace”](#) on page 893
- [“show ipv6 ospf database inter-prefix”](#) on page 894
- [“show ipv6 ospf database inter-router”](#) on page 895
- [“show ipv6 ospf database intra-prefix”](#) on page 896
- [“show ipv6 ospf database link”](#) on page 897
- [“show ipv6 ospf database network”](#) on page 898
- [“show ipv6 ospf database router”](#) on page 900
- [“show ipv6 ospf interface”](#) on page 905
- [“show ipv6 ospf neighbor”](#) on page 906
- [“show ipv6 ospf route”](#) on page 907
- [“show ipv6 ospf virtual-links”](#) on page 908

- [“summary-address \(IPv6 OSPF\)”](#) on page 909
- [“timers spf exp \(IPv6 OSPF\)”](#) on page 911
- [“undebg ipv6 ospf events”](#) on page 912
- [“undebg ipv6 ospf ifsm”](#) on page 913
- [“undebg ipv6 ospf lsa”](#) on page 914
- [“undebg ipv6 ospf nfsm”](#) on page 915
- [“undebg ipv6 ospf packet”](#) on page 916
- [“undebg ipv6 ospf route”](#) on page 917

abr-type

Overview Use this command to set an OSPF Area Border Router (ABR) type.

Use the **no** variant of this command to revert the ABR type to the default setting (cisco).

Syntax `abr-type {cisco|ibm|standard}`
`no abr-type [cisco|ibm|standard]`

Parameter	Description
cisco	Specifies an alternative ABR using Cisco implementation (RFC 3509). This is the default ABR type.
ibm	Specifies an alternative ABR using IBM implementation (RFC 3509).
standard	Specifies a standard behavior ABR (RFC 2328).

Default ABR type cisco

Mode Router Configuration

Usage notes Specifying the ABR type allows better interoperability between different implementations. This command is specially useful in a multi-vendor environment. The different ABR types are:

- Cisco ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached and one of them is the backbone area.
- IBM ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case the configured backbone need not be actively connected.
- Standard ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached to it.

Example To set the ABR type to **ibm** use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# abr-type ibm
```

area authentication ipsec spi

Overview Use this command in Router Configuration mode to enable either MD5 (Message-Digest 5) or SHA1 (Secure Hash Algorithm 1) authentication for a specified OSPF area.

Use the **no** variant of this command in Router Configuration mode to disable the authentication configured for a specified OSPF area.

Syntax `area <area-id> authentication ipsec spi <256-4294967295> {md5 <MD5-key>|sha1 <SHA1-key>}`
`no area <area-id> authentication ipsec spi <256-4294967295>`

Parameter	Description
<area-id>	The OSPF area that you are specifying the summary route default-cost for. This can be entered in either dotted decimal format or normal decimal format. Use one of the following formats:
	<ip-addr> OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295> OSPF area-ID expressed as a decimal number within the range shown.
	For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.
md5	Specify the MD5 (Message-Digest 5) hashing algorithm.
<MD5-key>	Enter an MD5 key containing up to 32 hexadecimal characters.
sha1	Specify the SHA-1 (Secure Hash Algorithm 1) hashing algorithm.
<SHA1-key>	Enter an SHA-1 key containing up to 40 hexadecimal characters.

Mode Router Configuration

Usage notes Use this command on an OSPFv3 area; use the [area virtual-link authentication ipsec spi](#) command on an OSPFv3 area virtual link. Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information and examples.

NOTE: You can configure an authentication security policy (SPI) on an OSPFv3 area with this command, or on an interface with the [ipv6 ospf authentication spi](#) command.

When you configure authentication for an area, the security policy is applied to all interfaces in the area. However, we recommend a different authentication security policy is applied to each interface for higher security.

If you apply the **ipv6 ospf authentication null** command, this affects authentication configured on both the interface and the OSPFv3 area.

This is due to OSPFv3 hello messages ingressing interfaces, which are part of area authentication, not being authenticated. So neighbors time out.

Example To enable MD5 authentication with a 32 hexadecimal character key for OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 authentication ipsec spi 1000 md5
1234567890ABCDEF1234567890ABCDEF
```

To enable SHA-1 authentication with a 40 hexadecimal character key for OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 authentication ipsec spi 1000
sha1 1234567890ABCDEF1234567890ABCDEF12345678
```

To disable authentication for OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 authentication ipsec spi 1000
```

Related commands

- [area encryption ipsec spi esp](#)
- [area virtual-link authentication ipsec spi](#)
- [area virtual-link encryption ipsec spi](#)
- [ipv6 ospf authentication spi](#)
- [ipv6 ospf encryption spi esp](#)
- [show ipv6 ospf](#)

area default-cost (IPv6 OSPF)

Overview This command specifies a cost for the default summary route sent into a stub area. The **no** variant of this command removes the assigned default-route cost.

Syntax `area <area-id> default-cost <0-16777215>`
`no area <area-id> default-cost`

Parameter	Description
<area-id>	The OSPF area that you are specifying the summary route default-cost for. This can be entered in either dotted decimal format or normal decimal format. Use one of the following formats:
	<ip-addr> OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295> OSPF area-ID expressed as a decimal number within the range shown.
	For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.
default-cost	Indicates the cost for the default summary route used for a stub area. Default: 1

Mode Router Configuration

Usage The default-cost option provides the metric for the summary default route, generated by the area border router, into the stub area. Use this option only on an area border router that is attached to the stub area.

Example To set the default cost to 10 in area 1 for the OSPF process P2, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf P2
awplus(config-router)# area 1 default-cost 10
```

Related commands [area stub \(IPv6 OSPF\)](#)

area encryption ipsec spi esp

Overview Use this command in Router Configuration mode to enable either AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) or 3DES (Triple Data Encryption Standard) ESP (Encapsulating Security Payload) encryption for a specified OSPF area.

Use the **no** variant of this command in Router Configuration mode to disable the encryption configured for a specified OSPF area.

Syntax `area <area-id> encryption ipsec spi <256-4294967295> esp
{aes-cbc <AES-CBC-key>|3des <3DES-key>|null}{md5
<MD5-key>|sha1 <SHA1-key>}
no area <area-id> encryption ipsec spi <256-4294967295>`

Parameter	Description				
<area-id>	The OSPF area that you are specifying the summary route default-cost for. This can be entered in either dotted decimal format or normal decimal format. Use one of the following formats: <table><tr><td><ip-addr></td><td>OSPF area-ID expressed in IPv4 address format A.B.C.D.</td></tr><tr><td><0-4294967295></td><td>OSPF area-ID expressed as a decimal number within the range shown.</td></tr></table> For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.	<ip-addr>	OSPF area-ID expressed in IPv4 address format A.B.C.D.	<0-4294967295>	OSPF area-ID expressed as a decimal number within the range shown.
<ip-addr>	OSPF area-ID expressed in IPv4 address format A.B.C.D.				
<0-4294967295>	OSPF area-ID expressed as a decimal number within the range shown.				
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.				
esp	Specify the esp keyword (Encapsulating Security Payload) to then apply either AES-CBC or 3DES encryption.				
aes-cbc	Specify this keyword to enable AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) encryption.				
<AES-CBC-key>	Enter an AES-CBC key containing either 32, 48, or 64 hexadecimal characters.				
3des	Specify 3DES (Triple Data Encryption Standard) encryption.				
<3DES-key>	Enter a 3DES key containing 48 hexadecimal characters.				
null	Specify ESP without AES-CBC or 3DES encryption applied.				
md5	Specify the MD5 (Message-Digest 5) encryption algorithm.				
<MD5-key>	Enter an MD5 key containing 32 hexadecimal characters.				
sha1	Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.				
<SHA1-key>	Enter an SHA-1 key containing 40 hexadecimal characters.				

Mode Router Configuration

Usage notes When you issue this command, authentication and encryption are both enabled.

Use this command on an OSPFv3 area, use the [area virtual-link encryption ipsec spi](#) command on an OSPFv3 area virtual link. Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

Security is achieved using the IPv6 ESP extension header. The IPv6 ESP extension header is used to provide confidentiality, integrity, authentication, and confidentiality. Authentication fields are removed from OSPF for IPv6 packet headers, so applying IPv6 ESP extension headers are required for integrity, authentication, and confidentiality.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information and examples.

NOTE: You can configure an encryption security policy (SPI) on an OSPFv3 area with this command, or on an interface with the [ipv6 ospf encryption spi esp](#) command.

When you configure encryption for an area, the security policy is applied to all interfaces in the area. However, we recommend a different encryption security policy is applied to each interface for higher security.

If you apply the **ipv6 ospf encryption null** command, this affects encryption configured on both the interface and the OSPFv3 area.

This is due to OSPFv3 hello messages ingressing interfaces, which are part of area encryption, not being encrypted. So neighbors time out.

Example To enable ESP encryption, but not apply an AES-CBC key or an 3DES key, and MD5 authentication with a 32 hexadecimal character key for OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 encryption ipsec spi 1000 esp null
md5 1234567890ABCDEF1234567890ABCDEF
```

To enable ESP encryption, but not apply an AES-CBC key or an 3DES key, and SHA-1 authentication with a 40 hexadecimal character key for OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 encryption ipsec spi 1000 esp null
sha1 1234567890ABCDEF1234567890ABCDEF12345678
```

To enable ESP encryption with a 48 hexadecimal character 3DES key and a 32 hexadecimal character MD5 authentication for OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 encryption ipsec spi 1000 esp 3des
1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF md5
1234567890ABCDEF1234567890ABCDEF
```

To enable ESP encryption with a 32 hexadecimal character AES-CBC key, and a 40 hexadecimal character SHA-1 authentication key for OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 encryption ipsec spi 1000 esp
aes-cbc 1234567890ABCDEF1234567890ABCDEF sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To disable ESP encryption for OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 encryption ipsec spi 1000
```

**Related
commands**

[area authentication ipsec spi](#)
[area virtual-link authentication ipsec spi](#)
[area virtual-link encryption ipsec spi](#)
[ipv6 ospf authentication spi](#)
[ipv6 ospf encryption spi esp](#)
[show ipv6 ospf](#)

area range (IPv6 OSPF)

Overview Use this command to summarize OSPFv3 routes at an area boundary, configuring an IPv6 address range which consolidates OSPFv3 routes. By default, this feature is not enabled.

A summary route created by this command is then advertised to other areas by the Area Border Routers (ABRs). In this way, routing information is condensed at area boundaries and outside the area so that routes are exchanged between areas in an efficient manner.

If the network numbers in an area are arranged into sets of contiguous routes, the ABRs can be configured to advertise a summary route that covers all the individual networks within the area that fall into the specified range.

The **no** variant of this command disables this function and restores default behavior.

Syntax `area <area-id> range <ipv6address/prefix-length> [advertise|not-advertise]`
`no area <area-id> range <ipv6address/prefix-length>`

Parameter	Description
<area-id>	The OSPFv3 area that you summarizing the routes for. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format.
	<A.B.C.D> OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295> OSPF area-ID expressed as a decimal number within the range shown.
	For example the values 0.0.1.2 and decimal 258 would both define the same area-ID.
<ip-addr/prefix-length>	The IPv6 address uses the format X:X::X/X/Prefix-Length. The prefix-length is usually set between 0 and 64.
advertise	Advertise this range as a summary route into other areas.
not-advertise	Do not advertise this range.

Default The area range is not configured by default. The area range is advertised if it is configured.

Mode Router Configuration

Usage notes You can configure multiple ranges on a single area with multiple instances of this command, so OSPFv3 summarizes addresses for different sets of IPv6 address ranges.

Ensure OSPFv3 IPv6 routes exist in the area range for advertisement before using this command.

Example awplus# configure terminal
awplus(config)# router ipv6 ospf P2
awplus(config-router)# area 1 range 2000::/3

area stub (IPv6 OSPF)

Overview This command defines an OSPF area as a stub area. By default, no stub area is defined.

Use this command when routers in the area do not require learning about external LSAs. You can define the area as a totally stubby area by configuring the Area Border Router of that area using the **area stub no-summary** command.

The **no** variant of this command removes this definition.

Syntax `area <area-id> stub [no-summary]`
`no area <area-id> stub [no-summary]`

Parameter	Description
<area-id>	The OSPF area that you are configuring as a stub area. Use one of the following formats: This can be entered in either dotted decimal format or normal decimal format. For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area-ID.
	<A.B.C.D> OSPF area-ID, expressed in the IPv4 address format <A.B.C.D>.
	<0-4294967295> OSPF area-ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area-ID.
no-summary	Stops an ABR from sending summary link advertisements into the stub area.

Mode Router Configuration

Usage There are two stub area router configuration commands: the **area stub** and **area default-cost** commands. In all routers attached to the stub area, configure the area by using the **area stub** command. For an area border router (ABR) attached to the stub area, also use the **area default-cost** command.

Example

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# area 100 stub
```

Related commands [area default-cost \(IPv6 OSPF\)](#)

area virtual-link (IPv6 OSPF)

Overview This command configures a link between a non-backbone area and the backbone, through other non-backbone areas.

In OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection.

The **no** variant of this command removes the virtual link.

Syntax

```
area <area-id> virtual-link <router-id>
no area <area-id> virtual-link <router-id>
area <area-id> virtual-link <router-id>
no area <area-id> virtual-link <router-id>
area <area-id> virtual-link <router-id> [hello-interval
<1-65535>] [retransmit-interval <1-65535>] [transmit-delay
<1-65535>]
no area <area-id> virtual-link <router-id> [hello-interval]
[retransmit-interval] [transmit-delay]
```

Parameter	Description
<area-id>	The area-ID of the transit area that the virtual link passes through. This can be entered in either dotted decimal format or normal decimal format as shown below.
	<A.B.C.D> OSPF area-ID, expressed in the IPv4 address format <A.B.C.D>.
	<0-4294967295> OSPF area-ID expressed as a decimal number within the range shown.
	For example the values dotted decimal 0.0.1.2 and decimal 258 would both define the same area-ID.
<router-id>	The OSPF router ID of the virtual link neighbor.
dead-interval	If no packets are received from a particular neighbor for dead-interval seconds, the router considers the neighbor router to be off-line. Default: 40 seconds
	<1-65535> The number of seconds in the interval.
hello-interval	The interval the router waits before it sends a hello packet. Default: 10 seconds
	<1-65535> The number of seconds in the interval.
retransmit-interval	The interval the router waits before it retransmits a packet. Default: 5 seconds
	<1-65535> The number of seconds in the interval.

Parameter	Description
transmit-delay	The interval the router waits before it transmits a packet. Default: 1 seconds
	<1-65535> The number of seconds in the interval.

Mode Router Configuration

Usage You can configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these two routers, joined by a virtual link, as if they were connected by an unnumbered point-to-point network. To configure a virtual link, you require:

- The transit area-ID, i.e. the area-ID of the non-backbone area that the two backbone routers are both connected to.
- The corresponding virtual link neighbor's router ID. To see the router ID use the [show ipv6 ospf](#) command.

Configure the **hello-interval** to be the same for all routers attached to a common network. A short **hello-interval** results in the router detecting topological changes faster but also an increase in the routing traffic.

The **retransmit-interval** is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The **transmit-delay** is the time taken to transmit a link state update packet on the interface. Before transmission, the link state advertisements in the update packet, are incremented by this amount. Set the **transmit-delay** to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

Example To configure a virtual link through area 1 to the router with router-ID 10.10.11.50, use the following commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# area 1 virtual-link 10.10.11.50 hello 5
dead 10
```

Related commands [show ipv6 ospf](#)

area virtual-link authentication ipsec spi

Overview Use this command in Router Configuration mode to enable authentication for virtual links in a specified OSPF area.

Use the **no** variant of this command in Router Configuration mode to disable authentication for virtual links in a specified OSPF area.

Syntax `area <area-id> virtual-link <router-ID> authentication ipsec spi <256-4294967295> {md5 <MD5-key>|sha1 <SHA1-key>}`
`no area <area-id> virtual-link <router-ID> authentication ipsec spi <256-4294967295>`

Parameter	Description
<area-id>	The OSPF area that you are specifying the summary route default-cost for. This can be entered in either dotted decimal format or normal decimal format. Use one of the following formats:
	<ip-addr> OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295> OSPF area-ID expressed as a decimal number within the range shown.
	For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.
virtual-link	Specify a virtual link and its parameters.
<router-ID>	Enter a router ID associated with a virtual link neighbor in IPv4 address format A.B.C.D.
authentication	Specify this keyword to enable authentication.
ipsec	Specify this keyword to use IPsec authentication.
spi	Specify this keyword to set the SPI (Security Parameters Index).
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.
md5	Specify the MD5 (Message-Digest 5) encryption algorithm.
<MD5-key>	Enter an MD5 key containing 32 hexadecimal characters.
sha1	Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.
<SHA1-key>	Enter an SHA-1 key containing 40 hexadecimal characters.

Mode Router Configuration

Usage notes Use this command on an OSPFv3 area virtual link, use the [area authentication ipsec spi](#) command on an OSPFv3 area. Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by

link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

OSPFv3 areas are connected to a backbone area. Virtual links can be configured to repair lost connections to a backbone area for OSPFv3 areas. To configure an OSPFv3 virtual link, use a router ID instead of the IPv6 prefix of the router.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information and examples.

Example To enable MD5 authentication with a 32 hexadecimal character key for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1
authentication ipsec spi 1000 md5
1234567890ABCDEF1234567890ABCDEF
```

To enable SHA-1 authentication with a 40 hexadecimal character key for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1
authentication ipsec spi 1000 sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To disable authentication for virtual links in OPSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 virtual-link ipsec spi 1000
```

Related commands

- [area authentication ipsec spi](#)
- [area encryption ipsec spi esp](#)
- [area virtual-link encryption ipsec spi](#)
- [show ipv6 ospf virtual-links](#)

area virtual-link encryption ipsec spi

Overview Use this command in Router Configuration mode to enable either AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) or 3DES (Triple Data Encryption Standard) ESP (Encapsulating Security Payload) encryption for virtual links in a specified OSPF area.

Use the **no** variant of this command in Router Configuration mode to disable encryption configured for virtual links in a specified OSPF area.

Syntax `area <area-id> virtual-link <router-ID> encryption ipsec spi <256-4294967295> esp {aes-cbc <AES-CBC-key>|3des <3DES-key>|null} {md5 <MD5-key>|sha1 <SHA1-key>}`
`no area <area-id> encryption ipsec spi <256-4294967295>`

Parameter	Description
<area-id>	The OSPF area that you are specifying the summary route default- cost for. This can be entered in either dotted decimal format or normal decimal format. Use one of the following formats:
	<ip-addr> OSPF area-ID expressed in IPv4 address format A.B.C.D.
	<0-4294967295> OSPF area-ID expressed as a decimal number within the range shown.
	For example, the values 0.0.1.2 and decimal 258 would both define the same area-ID.
virtual-link	Specify a virtual link and its parameters.
<router-ID>	Enter a router ID associated with a virtual link neighbor in IPv4 address format A.B.C.D.
encryption	Specify this keyword to enable encryption.
ipsec	Specify this keyword to use IPsec authentication.
spi	Specify this keyword to set the SPI (Security Parameters Index).
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.
esp	Specify the esp keyword (Encapsulating Security Payload) to then apply either AES-CBC or 3DES encryption.
aes-cbc	Specify this keyword to enable AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) encryption.
<AES-CBC-key>	Enter an AES-CBC key containing either 32, 48, or 64 hexadecimal characters.
3des	Specify 3DES (Triple Data Encryption Standard) encryption.
<3DES-key>	Enter a 3DES key containing 48 hexadecimal characters.

Parameter	Description
null	Specify ESP without AES-CBC or 3DES encryption applied.
md5	Specify the MD5 (Message-Digest 5) encryption algorithm.
<MD5-key>	Enter an MD5 key containing 32 hexadecimal characters.
sha1	Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.
<SHA1-key>	Enter an SHA-1 key containing 40 hexadecimal characters.

Mode Router Configuration

Usage notes When you issue this command, authentication and encryption are both enabled.

Use this command on an OSPFv3 area virtual link, use the [area encryption ipsec spi esp](#) command on an OSPFv3 area. Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

Security is achieved using the IPv6 ESP extension header. ESP is used to provide confidentiality, integrity, authentication, and confidentiality. Authentication fields are removed from OSPF for IPv6 packet headers. The IPv6 ESP extension header is required for integrity, authentication, and confidentiality.

Note that interface configuration takes priority over area configuration. If an interface configuration is removed then an area configuration is applied to an interface instead.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information and examples.

Example To enable ESP encryption, but not apply an AES-CBC key or a 3DES key, and MD5 authentication with a 32 hexadecimal character key for virtual links in OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption
ipsec spi 1000 esp null md5 1234567890ABCDEF1234567890ABCDEF
```

To enable ESP encryption, but not apply an AES-CBC key or a 3DES key, and SHA-1 authentication with a 40 hexadecimal character key for virtual links in OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption
ipsec spi 1000 esp null sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To enable ESP encryption with a 32 hexadecimal character AES-CBC key and a 40 hexadecimal character SHA-1 authentication key for virtual links in OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption
ipsec spi 1000 esp aes-cbc 1234567890ABCDEF1234567890ABCDEF
sha1 1234567890ABCDEF1234567890ABCDEF12345678
```

To enable ESP encryption with a 48 hexadecimal character 3DES key and a 40 hexadecimal character SHA-1 authentication key for virtual links in OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# area 1 virtual-link 10.0.0.1 encryption
ipsec spi 1000 esp 3des
1234567890ABCDEF1234567890ABCDEF1234567890ABCDEF sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To disable authentication for virtual links in OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no area 1 virtual-link 10.0.0.1
authentication ipsec spi 1000
```

**Related
commands**

[area authentication ipsec spi](#)
[area encryption ipsec spi esp](#)
[area virtual-link authentication ipsec spi](#)
[show ipv6 ospf virtual-links](#)

auto-cost reference bandwidth (IPv6 OSPF)

Overview This command controls how OSPF calculates default metrics for the interface. Use the **no** variant of this command to assign cost based only on the interface bandwidth.

Syntax `auto-cost reference-bandwidth <1-4294967>`
`no auto-cost reference-bandwidth`

Parameter	Description
<code><1-4294967></code>	The reference bandwidth, measured in Mbits per second (Mbps).

Default 1000 Mbps

Usage notes By default, OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the interface bandwidth. The default for the reference bandwidth is 1000 Mbps. As a result, if this default is used, there is very little difference between the metrics applied to interfaces of increasing bandwidth beyond 1000 Mbps.

The auto-cost command is used to alter this reference bandwidth in order to give a real difference between the metrics of high bandwidth links of differing bandwidths. In a network that has multiple links with high bandwidths, specify a larger reference bandwidth value to differentiate the costs on those links.

Cost is calculated by dividing the reference bandwidth (Mbps) by the layer 3 interface (Switched Virtual Interface (SVI), Loopback or Ethernet interface) bandwidth. Interface bandwidth may be altered by using the [bandwidth](#) command as the SVI does not auto-detect the bandwidth based on the speed of associated device ports.

When the reference bandwidth calculation results in a cost integer greater than 1 but contains a fractional value (the value after the decimal point), the result rounds down to the nearest integer. The following example shows how the cost is calculated.

The reference bandwidth is 1000 Mbps and the interface bandwidth is 7 Mbps.

Calculation = $1000/7$

Calculation result = 142.85 (integer of 142, fractional value of 0.85)

Result after rounding down to the nearest integer = 142 (Interface cost is 142)

When the reference bandwidth calculation results in a cost less than 1, it is rounded up to the nearest integer which is 1. The following example shows how the cost is calculated.

The reference bandwidth is 1000 Mbps and the interface bandwidth is 10000 Mbps.

Calculation = $1000/10000$

Calculation result = 0.1

Result after rounding up to the nearest integer = 1 (Interface cost is 1)

The auto-cost reference bandwidth value should be consistent across all OSPF routers in the OSPF process.

Note that using the `ipv6 ospf cost` command on a layer 3 interface will override the cost calculated by this command.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 20
awplus(config-router)# auto-cost reference-bandwidth 1000
```

Related commands `ipv6 ospf cost`

bandwidth

Overview Use this command to specify the maximum bandwidth to be used for each interface. The bandwidth value is in bits per second. OSPF uses this to calculate metrics for the interface.

The **no** variant of this command removes any applied bandwidth value.

Syntax `bandwidth <bandwidth-setting>`
`no bandwidth`

Parameter	Description
<code><bandwidth-setting></code>	Sets the bandwidth for the interface. Enter a value in the range 1 to 10000000000 bits per second. Note that to avoid entering many zeros, you can add k, m, or g to internally add 3, 6 or 9 zeros to the number entered. For example entering 1k is the same as entering 1000.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Example To set the bandwidth on eth1 to be 10 Mbps, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# bandwidth 10000000
or
awplus(config-if)# bandwidth 10m
```

Related commands [show interface](#)

clear ipv6 ospf process

Overview This command clears and restarts the IPv6 OSPF routing process. Specify the Process ID to clear one particular OSPF process. When no Process ID is specified, this command clears all running OSPF processes.

Syntax `clear ipv6 ospf [<0-65535>] process`

Parameter	Description
<0-65535>	The routing process ID.

Mode Privileged Exec

Example `awplus# clear ipv6 ospf process`

debug ipv6 ospf events

Overview This command enables IPv6 OSPF debugging for event troubleshooting.

To enable all debugging options, specify **debug ipv6 ospf event** with no additional parameters.

The **no** and **undebug** variants of this command disable OSPF debugging. Using this command with no parameters entered, will disable debugging for all parameter options.

Syntax `debug ipv6 ospf events [abr] [asbr] [os][router] [vlink]`
`no debug ipv6 ospf events [abr] [asbr] [os] [router] [vlink]`

Parameter	Description
abr	Shows ABR events.
asbr	Shows ASBR events.
router	Shows other router events.
os	Shows OS events.
vlink	Shows virtual link events.

Mode Privileged Exec and Global Configuration

Example To enable IPv6 event debugging and show ABR events, use the following command:

```
awplus# debug ipv6 ospf events asbr
```

debug ipv6 ospf ifsm

- Overview** This command specifies debugging options for IPv6 OSPF Interface Finite State Machine (IFSM) troubleshooting.
- To enable all debugging options, specify **debug ipv6 ospf ifsm** with no additional parameters.
- The **no** and **undebug** variants of this command disable IPv6 OSPF IFSM debugging. Use these commands without parameters to disable all the options.

Syntax debug ipv6 ospf ifsm [events] [status] [timers]
no debug ipv6 ospf ifsm [events] [status] [timers]

Parameter	Description
events	Displays IFSM event information.
status	Displays IFSM status information.
timers	Displays IFSM timer information.

Mode Privileged Exec and Global Configuration

Example To specify IPv6 OSPF debugging options to display IPv6 OSPF IFSM events information, use the following commands:

```
awplus# debug ipv6 ospf ifsm events
```

Related commands [terminal monitor](#)
[undebug ipv6 ospf ifsm](#)

debug ipv6 ospf lsa

Overview This command enables debugging options for IPv6 OSPF Link State Advertisements (LSA) troubleshooting. This displays information related to internal operations of LSAs.

To enable all debugging options, specify **debug ipv6 ospf lsa** with no additional parameters.

The **no** and **undebug** variants of this command disable IPv6 OSPF LSA debugging. Use this command without parameters to disable all the options.

Syntax

```
debug ipv6 ospf lsa [flooding] [generate] [install] [maxage] [refresh]
no debug ipv6 ospf lsa [flooding] [generate] [install] [maxage] [refresh]
```

Parameter	Description
<code>flooding</code>	Displays LSA flooding.
<code>generate</code>	Displays LSA generation.
<code>install</code>	Show LSA installation.
<code>maxage</code>	Shows maximum age of the LSA in seconds.
<code>refresh</code>	Displays LSA refresh.

Mode Privileged Exec and Global Configuration

Examples To enable debugging for IPv6 OSPF refresh LSA, use the following commands:

```
awplus# debug ipv6 ospf lsa refresh
```

Related commands [terminal monitor](#)
[undebug ipv6 ospf lsa](#)

debug ipv6 ospf nfsm

Overview This command enables debugging options for IPv6 OSPF Neighbor Finite State Machines (NFSMs).

To enable all debugging options, specify **debug ipv6 ospf nfsm** with no additional parameters.

The **no** and **undebug** variants of this command disable IPv6 OSPF NFSM debugging. Use this command without parameters to disable all the options.

Syntax `debug ipv6 ospf nfsm [events] [status] [timers]`
`no debug ipv6 ospf nfsm [events] [status] [timers]`

Parameter	Description
events	Displays NFSM event information.
status	Displays NFSM status information.
timers	Displays NFSM timer information.

Mode Privileged Exec and Global Configuration

Examples To enable IPv6 debugging option to display timer information, use the following command:

```
awplus# debug ipv6 ospf nfsm timers
```

Related commands [terminal monitor](#)
[undebug ipv6 ospf nfsm](#)

debug ipv6 ospf packet

Overview This command enables debugging options for IPv6 OSPF packets.

To enable all debugging options, specify **debug ipv6 ospf packet** with no additional parameters.

The **no** and **undebug** variants of this command disable IPv6 OSPF packet debugging. Use this command without parameters to disable all options.

Syntax

```
debug ipv6 ospf packet [dd] [detail] [hello] [ls-ack]
[ls-request] [ls-update] [recv] [send]

no debug ipv6 ospf packet [dd] [detail] [hello] [ls-ack]
[ls-request] [ls-update] [recv] [send]
```

Parameter	Description
dd	Specifies debugging for IPv6 OSPF database descriptions.
detail	Sets the debug option to detailed information.
hello	Specifies debugging for IPv6 OSPF hello packets.
ls-ack	Specifies debugging for IPv6 OSPF link state acknowledgments.
ls-request	Specifies debugging for IPv6 OSPF link state requests.
ls-update	Specifies debugging for IPv6 OSPF link state updates.
recv	Specifies the debug option set for received packets.
send	Specifies the debug option set for sent packets.

Mode Privileged Exec and Global Configuration

Examples To enable debugging for hello packets, use the following command:

```
awplus# debug ipv6 ospf packet hello
```

Related commands

- [terminal monitor](#)
- [undebug ipv6 ospf packet](#)

debug ipv6 ospf route

Overview This command enables debugging of route calculation. Use this command without parameters to turn on all the options.

The **no** and **undebug** variants of this command disable IPv6 OSPF route debugging. Use this command without parameters to disable all options.

Syntax `debug ipv6 ospf route [ase] [ia] [install] [spf]`
`no debug ipv6 ospf route [ase] [ia] [install] [spf]`

Parameter	Description
ase	Specifies the debugging of external route calculation.
ia	Specifies the debugging of inter-area route calculation.
install	Specifies the debugging of route installation.
spf	Specifies the debugging of SPF calculation.

Mode Privileged Exec and Global Configuration

Examples To enable IPv6 route debugging of inter-area route calculations, use the following command:

```
awplus# debug ipv6 ospf route ia
```

Related commands [terminal monitor](#)
[undebug ipv6 ospf route](#)

default-information originate

Overview This command creates a default external route into an OSPF routing domain.

When you use the **default-information originate** command to redistribute routes into an OSPF routing domain, then the system acts like an Autonomous System Boundary Router (ASBR). By default, an ASBR does not generate a default route into the OSPF routing domain.

When using this command, also specify the **route-map** *<route-map>* option to avoid a dependency on the default network in the routing table.

The **metric-type** is an external link type associated with the default route advertised into the OSPF routing domain. The value of the external route could be either Type 1 or 2. The default is Type 2.

The **no** variant of this command disables this feature.

Syntax

```
default-information originate [always] [metric <metric>]
[metric-type <1-2>] [route-map <route-map>]

no default-information originate [always] [metric]
[metric-type] [route-map]
```

Parameter	Description
always	Used to advertise the default route regardless of whether there is a default route.
<metric>	The metric value used in creating the default route. Enter a value in the range 0 to 16777214. The default metric value is 10. The value used is specific to the protocol.
<1-2>	External metric type for default routes, either OSPF External Type 1 or Type 2 metrics. Enter the value 1 or 2.
route-map	Specifies to use a specific route-map.
<route-map>	The route-map name. It is a string comprised of any characters, numbers or symbols.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router ospf 100
awplus(config-router)# default-information originate always
metric 23 metric-type 2 route-map myinfo
```

Related commands [route-map](#)

default-metric (IPv6 OSPF)

Overview This command sets default metric value for routes redistributed into the IPv6 OSPF routing protocol.

The **no** variant of this command returns IPv6 OSPF to using built-in, automatic metric translations, as appropriate for each routing protocol.

Syntax `default-metric <0-16777214>`
`no default-metric [<0-16777214>]`

Parameter	Description
<code><1-16777214></code>	Default metric value appropriate for the specified routing protocol.

Mode Router Configuration

Usage notes A default metric facilitates redistributing routes even with incompatible metrics. If the metrics do not convert, the default metric provides an alternative and enables the redistribution to continue. The effect of this command is that IPv6 OSPF will use the same metric value for **all** redistributed routes. Use this command in conjunction with the [redistribute \(IPv6 OSPF\)](#) command.

Examples

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# default-metric 100
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# no default-metric
```

Related commands [redistribute \(IPv6 OSPF\)](#)

distance (IPv6 OSPF)

Overview This command sets the administrative distance for OSPFv3 routes based on the route type. Your device uses this value to select between two or more routes to the same destination from two different routing protocols. The route with the smallest administrative distance value is added to the Forwarding Information Base (FIB). See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information.

Use the command **distance ospfv3** to set the distance for an entire category of OSPFv3 routes, rather than the specific routes that pass an access list.

Use the command **distance <1-254>**, with no other parameter, to set the same distance for all OSPFv3 route types.

The **no** variant of this command sets the administrative distance for OSPFv3 routes to the default of 110.

Syntax `distance <1-254>`
`distance ospfv3 {external <1-254>|inter-area <1-254>|intra-area <1-254>}`
`no distance {ospfv3|<1-254>}`

Parameter	Description
<1-254>	Specify the Administrative Distance value for OSPFv3 routes.
external	Sets the distance for routes from other routing domains, learned by redistribution. Specify an OSPFv3 external distance in the range <1-254>.
inter-area	Sets the distance for all routes from one area to another area. Specify an OSPFv3 inter-area distance in the range<1-254>.
intra-area	Sets the distance for all routes within an area. Specify an OSPFv3 intra-area distance in the range <1-254>.

Default The default OSPFv3 administrative distance is 110. The default Administrative Distance for each type of route (intra, inter, or external) is 110.

Mode Router Configuration

Usage notes The administrative distance rates the trustworthiness of a routing information source. The distance could be any integer from 0 to 254. A higher distance value indicates a lower trust rating. For example, an administrative distance of 254 indicates that the routing information source cannot be trusted and should be ignored.

Use this command to set the distance for an entire group of routes, rather than a specific route that passes an access list.

Examples To set the following administrative distances for route types in OSPF 100:

- 20 for inter-area routes

- 10 for intra-area routes
- 40 for external routes

use the commands:

```
awplus(config)# router ipv6 ospf 100
```

```
awplus(config-router)# distance ospfv3 inter-area 20 intra-area  
10 external 40
```

To set the administrative distance for all routes in OSPFv3 100 back to the default of 110, use the commands:

```
awplus(config)# router ipv6 ospf 100
```

```
awplus(config-router)# no distance ospfv3
```

ipv6 ospf authentication spi

Overview Use this command in Interface Configuration mode to enable either MD5 (Message-Digest 5) or SHA1 (Secure Hash Algorithm 1) authentication for a specified interface.

Use the **no** variant of this command in Interface Configuration mode to disable the authentication configured for a specified interface.

Syntax `ipv6 ospf authentication ipsec spi <256-4294967295> {md5 <MD5-key>|sha1 <SHA1-key>}`
`ipv6 ospf authentication null`
`no ipv6 ospf authentication ipsec spi <256-4294967295>`

Parameter	Description
authentication	Specify this keyword to enable authentication.
ipsec	Specify this keyword to use IPsec authentication.
spi	Specify this keyword to set the SPI (Security Parameters Index).
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.
md5	Specify the MD5 (Message-Digest 5) hashing algorithm.
<MD5-key>	Enter an MD5 key containing up to 32 hexadecimal characters.
sha1	Specify the SHA-1 (Secure Hash Algorithm 1) hashing algorithm.
<SHA1-key>	Enter an SHA-1 key containing up to 40 hexadecimal characters.
null	Specify no authentication is applied when no other parameters are applied after this keyword (<code>ipv6 ospf authentication null</code>). Note this overrides any existing area authentication configured.

Default Authentication is not configured on an interface by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes Configure the same SPI (Security Parameters Index) value on all interfaces that connect to the same link. SPI values are used by link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

Use the **null** keyword to override existing area authentication. Apply the **null** keyword if area authentication is already configured to configure authentication on an interface.

See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information and examples.

NOTE: You can configure an authentication security policy (SPI) on an interface with this command, or an OSPFv3 area with the [area authentication ipsec spi](#) command.

When you configure authentication for an area, the security policy is applied to all interfaces in the area. Allied Telesis recommends a different authentication security policy is applied to each interface for higher security.

If you apply the **ipv6 ospf authentication null** command, this affects authentication configured on both the interface and the OSPFv3 area.

This is due to OSPFv3 hello messages ingressing interfaces, which are part of area authentication, not being authenticated. So neighbors time out.

Example To enable SHA-1 authentication with a 40 hexadecimal character key for interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf authentication ipsec spi 1000 sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To specify no authentication is applied to interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf authentication null
```

To disable authentication for interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 ospf authentication ipsec spi 1000
```

Related commands

- [area authentication ipsec spi](#)
- [area encryption ipsec spi esp](#)
- [ipv6 ospf encryption spi esp](#)
- [show ipv6 ospf interface](#)

ipv6 ospf cost

Overview This command explicitly specifies the cost of the link-state metric in a router-LSA. The interface cost indicates the overhead required to send packets across a certain interface. Use this command to set the interface cost manually. The **no** variant of this command resets the interface cost to the default.

Syntax `ipv6 ospf cost <1-65535>`
`no ipv6 ospf cost`

Parameter	Description
<1-65535>	The link-state metric.

Default By default there is no static value set and the OSPF cost is automatically calculated by using the command [auto-cost reference bandwidth \(IPv6 OSPF\)](#).

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command explicitly sets a user specified cost of sending packets out the interface. Using this command overrides the cost value calculated automatically with the auto-cost reference bandwidth (IPv6 OSPF) feature.

The link-state metric cost is stated in the Router-LSA's link. Typically, the cost is inversely proportional to the bandwidth of an interface. By default, the cost of an interface is calculated according to the following formula:

$$\text{reference bandwidth} / \text{interface bandwidth}$$

The reference bandwidth is set by default at 1000000 kbps (or 1000 Mbps), but can be changed by the command [auto-cost reference bandwidth \(IPv6 OSPF\)](#).

The interface bandwidth is set by default to 1000000 kbps (or 1000 Mbps), but can be changed by the [bandwidth](#) command.

Example To set the IPv6 OSPF cost to 10 on the interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 ospf cost 10
```

Related commands [show ipv6 ospf interface](#)
[auto-cost reference bandwidth \(IPv6 OSPF\)](#)
[bandwidth](#)

ipv6 ospf dead-interval

Overview This command sets the interval during which no hello packets are received and after which a neighbor is declared dead.

The dead-interval is the amount of time that OSPF waits to receive an OSPF hello packet from the neighbor before declaring the neighbor is down. This value is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

The **no** variant of this command returns the interval to the default of 40 seconds.

Syntax `ipv6 ospf dead-interval <1-65535> [<inst-id>]`
`no ipv6 ospf dead-interval`

Parameter	Description
<1-65535>	The interval in seconds. Default: 40
<inst-id>	The instance ID Default: 0

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Default 40 seconds.

Example The following example shows configuring the dead-interval to 10 seconds on the interface eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf dead-interval 10
```

Related commands [ipv6 ospf hello-interval](#)
[show ipv6 ospf interface](#)

ipv6 ospf display route single-line

Overview Use this command to change the result of the **show ipv6 route** command to display each route entry on a single line.

Syntax `ipv6 ospf display route single-line`
`no ipv6 ospf display route single-line`

Mode Global Configuration

Example To display each route entry on a single line.

```
awplus# configure terminal
awplus(config)# ipv6 ospf display route single-line
```

Related commands [show ipv6 ospf route](#)

ipv6 ospf encryption spi esp

Overview Use this command in Interface Configuration mode to enable either AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) or 3DES (Triple Data Encryption Standard) ESP (Encapsulating Security Payload) encryption for a specified interface.

Use the **no** variant of this command in Interface Configuration mode to disable the encryption configured for a specified interface.

Syntax `ipv6 ospf encryption ipsec spi <256-4294967295> esp {aes-cbc <AES-CBC-key>|3des <3DES-key>|null} {md5 <MD5-key>|sha1 <SHA1-key>}`
`ipv6 ospf encryption null`
`no ipv6 ospf encryption ipsec spi <256-4294967295>`

Parameter	Description
<256-4294967295>	Specify an SPI (Security Parameters Index) value in the range 256 to 4294967295, entered as a decimal integer.
esp	Specify the esp keyword (Encapsulating Security Payload) to then apply either AES-CBC or 3DES encryption.
aes-cbc	Specify this keyword to enable AES-CBC (Advanced Encryption Standard-Cipher Block Chaining) encryption.
<AES-CBC-key>	Enter an AES-CBC key containing either 32, 48, or 64 hexadecimal characters.
3des	Specify 3DES (Triple Data Encryption Standard) encryption.
<3DES-key>	Enter a 3DES key containing 48 hexadecimal characters.
null	Specify ESP without AES-CBC or 3DES encryption applied.
md5	Specify the MD5 (Message-Digest 5) encryption algorithm.
<MD5-key>	Enter an MD5 key containing 32 hexadecimal characters.
sha1	Specify the SHA-1 (Secure Hash Algorithm 1) encryption algorithm.
<SHA1-key>	Enter an SHA-1 key containing 40 hexadecimal characters.
null	Specify no encryption is applied when no other parameters are applied after this keyword (<code>ipv6 ospf encryption null</code>).

Default Authentication is not configured on an interface by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes When you issue this command, authentication and encryption are both enabled. Configure the same SPI (Security Parameters Index) value on all interfaces that

connect to the same link. SPI values are used by link interfaces. Use a different SPI value for a different link interface when using OSPFv3 with link interfaces.

Security is achieved using the IPv6 ESP extension header. The IPv6 ESP extension header is used to provide confidentiality, integrity, authentication, and confidentiality. Authentication fields are removed from OSPF for IPv6 packet headers, so applying IPv6 ESP extension headers are required for integrity, authentication, and confidentiality.

Use the **null** keyword to override existing area encryption. Apply the **null** keyword if area encryption is already configured to then configure encryption on an interface instead.

Use the **sha1** keyword to choose SHA-1 authentication instead of entering the **md5** keyword to use MD5 authentication. The SHA-1 algorithm is more secure than the MD5 algorithm. SHA-1 uses a 40 hexadecimal character key instead of a 32 hexadecimal character key as used for MD5 authentication.

See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information and examples.

NOTE: You can configure an encryption security policy (SPI) on an interface with this command, or an OSPFv3 area with the [area encryption ipsec spi esp](#) command.

When you configure encryption for an area, the security policy is applied to all interfaces in the area. Allied Telesis recommends a different encryption security policy is applied for each interface for higher security.

If you apply the **ipv6 ospf encryption null** command this affects encryption configured on both the interface and the OSPFv3 area.

This is due to OSPFv3 hello messages ingressing interfaces, which are part of area encryption, not being encrypted. So neighbors time out.

Example To enable ESP encryption but not apply an AES-CBC key or a 3DES key, for interface eth1 and SHA-1 authentication with a 40 hexadecimal character key, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf encryption ipsec spi 1000 esp null
sha1 1234567890ABCDEF1234567890ABCDEF12345678
```

To enable ESP encryption with an AES-CBC key with a 32 hexadecimal character key and SHA-1 authentication with a 40 hexadecimal character key for interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf encryption ipsec spi 1000 esp
aes-cbc 1234567890ABCDEF1234567890ABCDEF sha1
1234567890ABCDEF1234567890ABCDEF12345678
```

To specify no ESP encryption is applied to interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf encryption null
```

To disable ESP encryption for interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 ospf encryption ipsec spi 1000
```

**Related
commands**

[area authentication ipsec spi](#)
[area encryption ipsec spi esp](#)
[ipv6 ospf authentication spi](#)
[show ipv6 ospf interface](#)

ipv6 ospf hello-interval

- Overview** This command specifies the interval between hello packets.
- The hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter interval ensures faster detection of topological changes, but results in more routing traffic.
- The **no** variant of this command returns the interval to the default of 10 seconds.

Syntax `ipv6 ospf hello-interval <1-65535>`
`no ipv6 ospf hello-interval`

Parameter	Description
<1-65535>	The hello-interval in seconds. Default: 10

- Default** The default interval is 10 seconds.
- Mode** Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.
- Example** The following example shows setting the hello-interval to 3 seconds on the interface eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf hello-interval 3
```

Related commands [ipv6 ospf dead-interval](#)
[show ipv6 ospf interface](#)

ipv6 ospf neighbor

Overview Use this command to configure static OSPFv3 IPv6 neighbors when using the OSPFv3 "non-broadcast" (NBMA) and "point-to-multipoint non-broadcast" (P2MP NBMA) network types. OSPFv3 messages exchanged between the neighbors are unicast only.

Use the **no** variant of this command to remove a configuration.

Syntax `ipv6 ospf neighbor <ipv6-address>
[<cost>|<instance-id>|<poll-interval>|<priority>]
no ipv6 ospf neighbor <ipv6-address>
[<cost>|<instance-id>|<poll-interval>|<priority>]`

Parameter	Description
<code><ipv6-address></code>	Specifies the interface IPv6 address of the neighbor.
<code><cost></code>	<i>cost</i> <1-65535> OSPF cost for point-to-multipoint neighbor.
<code><instance-id></code>	<i>instance-id</i> <0-255> Interface instance ID.
<code><poll-interval></code>	<i>poll-interval</i> <0-4294967295> Dead neighbor polling interval in seconds. It is recommended to set this value much higher than the hello interval. The default is 120 seconds.
<code><priority></code>	<i>priority</i> <0-255> Specifies the router priority value of the non-broadcast neighbor associated with the specified IP address. The default is 0. This keyword does not apply to point-to-multipoint interfaces.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes To configure a neighbor on an NBMA network manually, use the **ipv6 ospf neighbor** command and include one neighbor entry for each known non-broadcast network neighbor. The IPv6 address used in this command is the neighbor's primary IPv6 address on the interface where that neighbor connects to the NBMA network.

The poll interval is the reduced rate at which routers continue to send hello packets, when a neighboring router has become inactive. Set the poll interval to be much larger than the hello interval.

Examples To configure a neighbor with a priority value, poll interval time, and cost, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf neighbor fe80::c:20:0:1 priority 1
poll-interval 90
awplus(config-router)# ipv6 ospf neighbor fe80::c:20:0:1 cost
15
```

Related commands [show ipv6 ospf neighbor](#)

ipv6 ospf network

Overview This command configures the OSPF network type to a type different from the default for the particular interface.

The **no** variant of this command returns the network type to the default for the particular interface.

Syntax `ipv6 ospf network {broadcast|non-broadcast|point-to-point|point-to-multipoint}`
`no ipv6 ospf network`

Parameter	Description
<code>broadcast</code>	Sets the network type to broadcast.
<code>non-broadcast</code>	Sets the network type to NBMA.
<code>point-to-multipoint</code>	Sets the network type to point-to-multipoint.
<code>point-to-point</code>	Sets the network type to point-to-point.

Default The default is the default type for the interface, e.g broadcast for eth interfaces.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes This command forces the interface network type to be the specified type. Depending on the network type, OSPF changes the behavior of the packet transmission and the link description in LSAs.

Example The following example shows setting the network type to point-to-point on the interface eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf network point-to-point
```

ipv6 ospf priority

Overview This command sets the router priority, which is a parameter used in the election of the designated router for the link.

The **no** variant of this command returns the router priority to the default of 1.

Syntax `ipv6 ospf priority <priority>`
`no ipv6 ospf priority`

Parameter	Description
<priority>	<0-255> Specifies the router priority of the interface. The larger the value, the greater the priority level. The value 0 defines that the device cannot become either the DR, or backup DR for the link.

Default The default priority is 1.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage Set the priority to help determine the OSPF Designated Router (DR) for a link. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, the router with the higher router ID takes precedence.

Routers with zero router priority values cannot become the designated or backup designated router.

Example The following example shows setting the OSPFv3 priority value to 3 on the interface eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf priority 3
```


ipv6 ospf retransmit-interval

Overview Use this command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

Use the **no** variant of this command to return to the default of 5 seconds.

Syntax `ipv6 ospf retransmit-interval <1-65535>`
`no ipv6 ospf retransmit-interval`

Parameter	Description
<code><1-65535></code>	Specifies the interval in seconds.

Default The default interval is 5 seconds.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgment. In case the router does not receive an acknowledgment during the set time (the retransmit interval value) it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.

Example The following example shows setting the OSPF retransmit interval to 6 seconds on the interface eth1:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf retransmit-interval 6
```

ipv6 ospf transmit-delay

Overview Use this command to set the estimated time it takes to transmit a link-state-update packet on the interface.

Use the **no** variant of this command to return to the default of 1 second.

Syntax `ipv6 ospf transmit-delay <1-65535>`
`no ipv6 ospf transmit-delay`

Parameter	Description
<code><1-65535></code>	Specifies the time, in seconds, to transmit a link-state update.

Default The default interval is 1 second.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Add transmission and propagation delays when setting the transmit delay value.

Example To set the IPv6 OSPF transmit delay time to 3 seconds on the interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 ospf transmit-delay 3
```

ipv6 router ospf area

Overview Use this command to enable IPv6 OSPF routing on an interface.
Use the **no** variant of this command to disable IPv6 OSPF routing on an interface.

Syntax `ipv6 router ospf area <area-id> [tag <process-id>] [instance <instance-id>]`
`no ipv6 router ospf area <area-id>`

Parameter	Description
<area-id>	The ID of the IPv6 OSPF routing area. Can be entered as either an IPv4 A.B.C.D address format, or as an unsigned integer in the range, 0 to 4294967295. Use either of the following forms when entering an area-ID: • area-id <A.B.C.D> where A.B.C.D is a number entered in IPv4 address format. • area-id <0 to 4294967295>.
<process-id>	The process tag denotes a separate router process. It can comprise any string of alphanumeric characters. Note that this tag is local to the router on which it is set and does not appear in any OSPF packets or LSA.
<instance-id>	The OSPF instance ID, entered as an integer between 0 and 255. This is the value that will appear in the instance field of the IPv6 OSPF hello packet.

Defaults IPv6 OSPF routing is disabled by default.

When enabling IPv6 OSPF routing:

- the process-tag will default to a null value if not set.
- the Instance ID defaults to 0 if not set.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a PPP interface, a bridge, or a tunnel.

Usage notes When enabling IPv6 OSPF routing on an interface, specifying the area-ID is mandatory, but the Process tag and Instance are optional.

See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information and examples.

Examples To enable IPv6 OSPF on interface eth1 in OSPF area 1, with a tag of 'PT2', and instance 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 router ospf area 1 tag PT2 instance-id 2
```

To disable IPv6 OSPF on interface eth1 and OSPF area 1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 router ospf area 1
```

max-concurrent-dd (IPv6 OSPF)

Overview Use this command to limit the number of neighbors that can be concurrently processed in the database exchange. The specified value limits the number of neighbors from all interfaces, not per interface.

Use the **no** variant of this command to have no limit on the maximum number of LSAs.

Syntax `max-concurrent-dd <max-neighbors>`
`no max-concurrent-dd`

Parameter	Description
<code><max-neighbors></code>	<code><1-65535></code> The maximum number of neighbors.

Mode Router Configuration

Usage notes This command is useful where bringing up several adjacencies on a router is affecting performance. In this situation, you can often enhance the system performance by limiting the number of neighbors that can be processed concurrently.

Example The following example sets the max-concurrent-dd value to allow only 4 neighbors to be processed at a time.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# max-concurrent-dd 4
```

Related commands [router ipv6 ospf](#)

passive-interface (IPv6 OSPF)

Overview Use this command to suppress the sending of Hello packets on a specified interface. If you use the **passive-interface** command without the optional parameters then all interfaces are put into passive mode.

Use the **no** variant of this command to allow the sending of Hello packets on all interfaces, or on the specified interface. If you use the **no** variant of this command without the optional parameters then all interfaces are removed from passive mode.

Syntax `passive-interface [<interface>]`
`no passive-interface [<interface>]`

Parameter	Description
<interface>	The name of the interface.

Mode Router Configuration

Usage Configure an interface to be passive if you wish its connected route to be treated as an OSPF route (rather than an AS-external route), but do not wish to actually exchange any OSPF packets via this interface.

Examples To configure passive interface mode on all interfaces, enter the following commands:

```
awplus(config)# router ipv6 ospf
awplus(config-router)# passive-interface
```

To configure passive interface mode on the local loopback interface, enter the following commands:

```
awplus(config)# router ipv6 ospf
awplus(config-router)# passive-interface lo
```

To remove passive interface mode from all interfaces, enter the following commands:

```
awplus(config)# router ipv6 ospf
awplus(config-router)# no passive-interface
```

redistribute (IPv6 OSPF)

Overview Use this command to redistribute routes from other routing protocols, static routes and connected routes into an IPv6 OSPF routing table.

Use the **no** variant of this command to disable this function.

Syntax `redistribute <protocol> [metric <0-16777214>] [metric-type {1|2}] [route-map <route-map-entry>]`
`no redistribute <protocol>`

Parameter	Description
<protocol>	The routing protocol to be redistributed, can be one of:
connected	Connected routes
rip	Routing Internet Protocol
static	Static Routes
metric	Specifies the external metric.
metric-type	Specifies the external metric-type, either type 1 or type 2. • For Metric Type 1: The best route is based on the external redistributed path cost plus the internal path cost presented by the native routing protocol. • For Metric Type 2: The best route is based only on the external redistributed path cost. The internal path cost is only used to break a "tie" situation between two identical external path costs.
route-map	The name of the specific route-map.

Default The default metric value for routes redistributed into OSPFv3 is 20. The metric can also be defined using the [set metric](#) command for a route map. Note that a metric defined using the [set metric](#) command for a route map overrides a metric defined with this command.

Mode Router Configuration

Usage notes You use this command to inject routes, learned from other routing protocols, into the OSPF domain to generate AS-external-LSAs. If a route-map is configured by this command, then that route-map is used to control which routes are redistributed and can set metric and tag values on particular routes.

The metric, metric-type, and tag values specified on this command are applied to any redistributed routes that are not explicitly given a different metric, metric-type, or tag value by the route map.

See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information about metrics, and about behavior when configured in route maps.

Note that this command does not redistribute the default route. To redistribute the default route, use the [default-information originate](#) command.

Example The following example shows the redistribution of RIP routes into the IPv6 OSPF routing table, with a metric of 10 and a metric type of 1.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# redistribute rip metric 10 metric-type 1
```


restart ipv6 ospf graceful

Overview Use this command to force the OSPFv3 process to restart. You may optionally specify a grace-period value. If a grace-period is not specified then a default value of 120 seconds is applied.

You should specify a grace-period value of 120 seconds or more. Low grace-period values may cause the graceful restart process on neighboring routers to terminate with routes missing.

Syntax `restart ipv6 ospf graceful [grace-period <1-1800>]`

Parameter	Description
grace-period	Specify the grace period.
<1-1800>	The grace period in seconds.

Default The default OSPF grace-period is 120 seconds.

Mode Privileged Exec

Usage notes After this command is executed, the OSPFv3 process immediately shuts down. It notifies the system that OSPF has performed a graceful shutdown. Routes installed by OSPF are preserved until the grace-period expires.

When a **restart ospf graceful** command is issued, the OSPF configuration is reloaded from the last saved configuration. Ensure you first enter the [copy running-config startup-config](#) command.

Example To restart OSPFv3, use the following commands:

```
awplus# copy running-config startup-config
awplus# restart ipv6 ospf graceful grace-period 200
```

To apply the default grace-period (120 seconds), use the following commands:

```
awplus# copy running-config startup-config
awplus# restart ipv6 ospf graceful
```

router ipv6 ospf

Overview Use this command to create or remove an IPv6 OSPF routing process, or to enter the Router Configuration mode to configure a specific IPv6 OSPF routing process. Use the **no** variant of this command to terminate an IPv6 OSPF routing process.

Use the **no** parameter with the **process-id** parameter, to terminate and delete a specific IPv6 OSPF routing process.

Syntax `router ipv6 ospf [<process-id>]`
`no router ipv6 ospf [<process-id>]`

Parameter	Description
<process-id>	A character string that identifies a routing process. If you do not specify the process-id a "null" process ID will be applied. Note that this will appear in show output as *null*. However you cannot select the null process by using the character string *null* as command entry characters.

Default No routing process is defined by default.

Mode Global Configuration

Usage notes The process ID enables you to run more than one OSPF session within the same router, then configure each session to a different router port. Note that this function is internal to the router, and other routers (neighbors) have no knowledge of these different processes. The hello and LSAs issued from each process will appear as if coming from a separate physical router.

To a large extent the requirement for multiple processes has been replaced by the ability within IPv6 OSPF of running simultaneous router instances.

The process ID of IPv6 OSPF is an optional parameter for the **no** variant of this command only. When removing all IPv6 OSPF processes on the device, you do not need to specify each Process ID, but when removing particular IPv6 OSPF processes, you must specify each Process ID to be removed.

For a description of processes and instances and their configuration relationships, see the [OSPFv3 Feature Overview and Configuration Guide](#).

Example This example shows the use of this command to enter Router Configuration mode.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf P100
awplus(config-router)#
```

router-id (IPv6 OSPF)

Overview Use this command to specify a router ID for the IPv6 OSPF process.
Use the **no** variant of this command to disable this function.

Syntax `router-id <router-id>`
`no router-id`

Parameter	Description
<code><router-id></code>	Specifies the router ID in IPv4 address format.

Mode Router Configuration

Usage Configure each router with a unique router-id. In an IPv6 OSPF router process that has active neighbors, a new router-id takes effect at the next reload or when you restart OSPF manually.

Example The following example shows a specified router ID 0.0.4.5.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# router-id 0.0.4.5
```

Related commands [show ipv6 ospf](#)

show debugging ipv6 ospf

Overview Use this command to see what debugging is turned on for OSPFv3.

For information on filtering and saving command output, see the [“Getting_Started with AlliedWare Plus” Feature Overview and Configuration_Guide](#).

Syntax `show debugging ipv6 ospf`

Mode User Exec and Privileged Exec

Example `awplus# show debugging ipv6 ospf`

Output Figure 23-1: Example output from the **show debugging ipv6 ospf** command

```
OSPFv3 debugging status:
OSPFv3 all packet detail debugging is on
OSPFv3 all IFSM debugging is on
OSPFv3 all NFSM debugging is on
OSPFv3 all LSA debugging is on
OSPFv3 all NSM debugging is on
OSPFv3 all route calculation debugging is on
OSPFv3 all event debugging is on
```

show ipv6 ospf

- Overview** Use this command in User Exec or Privileged Exec modes to display general information about all IPv6 OSPF routing processes, including OSPFv3 Authentication configuration and status information.
- Include the process ID parameter with this command to display information about specified processes.
- For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Syntax** `show ipv6 ospf`
`show ipv6 ospf <process-id>`

Parameter	Description
<process-id>	<0-65535> The ID of the router process for which information will be displayed. If this parameter is included, only the information for the specified routing process is displayed.

- Mode** User Exec and Privileged Exec

- Examples** To display general information about all IPv6 OSPF routing processes, use the command:
- ```
awplus# show ipv6 ospf
```
- To display general information about IPv6 OSPF (OSPFv3) routing process P10, use the command:
- ```
awplus# show ipv6 ospf P10
```

Output Figure 23-2: Example output from the **show ipv6 ospf** command for process P10, showing OSPFv3 Authentication configuration information highlighted in bold

```
awplus#show ipv6 ospf
  Routing Process "OSPFv3 (10)" with ID 192.168.1.2
  Route Licence: Route : Limit=Unlimited, Allocated=0, Visible=0,
Internal=0
  Route Licence: Breach: Current=0, Watermark=0
  Process uptime is 6 minutes
  Current grace period is 120 secs (default)
  SPF schedule delay min 0.500 secs, SPF schedule delay max 50.0
secs
  Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
  Number of incoming current DD exchange neighbors 0/5
  Number of outgoing current DD exchange neighbors 0/5
  Number of external LSA 0. Checksum Sum 0x0000
  Number of AS-Scoped Unknown LSA 0
  Number of LSA originated 4
  Number of LSA received 10
  Number of areas in this router is 1
    Area BACKBONE(0)
      Number of interfaces in this area is 1(1)
      MD5 Authentication SPI 1000
      NULL Encryption SHA-1 Auth, SPI 1001
      SPF algorithm executed 9 times
      Number of LSA 3. Checksum Sum 0xF9CC
      Number of Unknown LSA 0
```

Related commands

- [area authentication ipsec spi](#)
- [area encryption ipsec spi esp](#)
- [router ipv6 ospf](#)

show ipv6 ospf database

Overview Use this command in User Exec or Privileged Exec modes to display a database summary for IPv6 OSPF information. Include the process ID parameter with this command to display information about specified processes.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf <process-id> database`
`[self-originate|max-age|adv router <adv-router-id>]`

Parameter	Description
<process-id>	<0-65535> The ID of the router process for which information will be displayed.
self-originate	Displays self-originated link states.
max-age	Displays LSAs in MaxAge list. It maintains the list of the all LSAs in the database which have reached the max-age which is 3600 seconds.
adv-router	Advertising Router LSA.
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.

Mode User Exec and Privileged Exec

Example To display the database summary for IPv6 OSPF information on process P10, use the command:

```
awplus# show ipv6 ospf P10 database
```

Output Figure 23-3: Example output from the **show ipv6 ospf P10 database** command

OSPFv3 Router with ID (0.0.1.1) (Process P10)						
Link-LSA (Interface eth1)						
Link State ID	ADV Router	Age	Seq#	CkSum	Prefix	
0.0.0.202	0.0.1.1	46	0x800000c3	0x5f50	1	
0.0.0.202	0.0.1.2	8	0x800000c3	0x4ca0	1	
...						

show ipv6 ospf database external

Overview Use this command in User Exec or Privileged Exec modes to display information about the external LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf database external <adv-router-id>
[self-originate|adv-router <adv-router-id>]`

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
self-originate	Self-originated link states.
adv-router	Displays all the LSAs of the specified router.

Mode User Exec and Privileged Exec

Examples To display information about the external LSAs, use the following command:

```
awplus# show ipv6 ospf database external adv-router 10.10.10.1
```

Output Figure 23-4: Example output from the **show ipv6 ospf database external** command

```
LS age: 1087
LS Type: AS-External-LSA
Link State ID: 0.0.0.13
Advertising Router: 0.0.1.1
LS Seq Number: 0x8000000C
Checksum: 0xCE9D
Length: 52
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 2010:2222::/64
  Prefix Options: 0 (-|-|-|-)
  Forwarding Address: 2003:1111::1
...
```


show ipv6 ospf database grace

Overview Use this command in User Exec or Privileged Exec modes to display information about the grace LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf database grace <adv-router-id>
[self-originate|adv-router <adv-router-id>]`

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
adv-router	Displays all the LSAs of the specified router.
self-originate	Self-originated link states.

Mode User Exec and Privileged Exec

Examples To display information about the grace LSAs, use the following command:

```
awplus# show ipv6 ospf database grace adv-router 10.10.10.1
```

Output Figure 23-5: Example output from the **show ipv6 ospf database grace** command

```
LS age: 1087
LS Type: AS-External-LSA
Link State ID: 0.0.0.13
Advertising Router: 0.0.1.1
LS Seq Number: 0x8000000C
Checksum: 0xCE9D
Length: 52
Metric Type: 2 (Larger than any link state path)
Metric: 20
Prefix: 2010:2222::/64
Prefix Options: 0 (-|-|-|-)
Forwarding Address: 2003:1111::1
```

show ipv6 ospf database inter-prefix

Overview Use this command in User Exec or Privileged Exec modes to display information about the inter-prefix LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf database inter-prefix <adv-router-id>
[self-originate|adv-router <adv-router-id>]`

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
adv-router	Displays all the LSAs of the specified router.
self-originate	Self-originated link states.

Mode User Exec and Privileged Exec

Examples To display information about the inter-prefix LSAs, use the following command:

```
awplus# show ipv6 ospf database external adv-router 10.10.10.1
```

Output Figure 23-6: Example output from the **show ipv6 ospf database inter-prefix** command

```
LS age: 1087
LS Type: AS-External-LSA
Link State ID: 0.0.0.13
Advertising Router: 0.0.1.1
LS Seq Number: 0x8000000C
Checksum: 0xCE9D
Length: 52
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 2010:2222::/64
  Prefix Options: 0 (-|-|-|-)
  Forwarding Address: 2003:1111::1
...
```

show ipv6 ospf database inter-router

Overview Use this command in User Exec or Privileged Exec modes to display information about the inter-router LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf database inter-router <adv-router-id>
[self-originate] adv-router <adv-router-id>]`

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
adv-router	Displays all the LSAs of the specified router.
self-originate	Self-originated link states.

Mode User Exec and Privileged Exec

Examples To display information about the inter-router LSAs, use the following command:

```
awplus# show ipv6 ospf database inter-router adv-router  
10.10.10.1
```

Output Figure 23-7: Example output from the **show ipv6 ospf database inter-router** command

```
LS age: 1087  
LS Type: AS-External-LSA  
Link State ID: 0.0.0.13  
Advertising Router: 0.0.1.1  
LS Seq Number: 0x8000000C  
Checksum: 0xCE9D  
Length: 52  
Metric Type: 2 (Larger than any link state path)  
Metric: 20  
Prefix: 2010:2222::/64  
Prefix Options: 0 (-|-|-|-)  
Forwarding Address: 2003:1111::1  
...
```

show ipv6 ospf database intra-prefix

Overview Use this command in User Exec or Privileged Exec modes to display information about the intra-prefix LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf database intra-prefix <adv-router-id>
[self-originate|adv-router <adv-router-id>]`

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
adv-router	Displays all the LSAs of the specified router.
self-originate	Self-originated link states.

Mode User Exec and Privileged Exec

Examples To display information about the intra-prefix LSAs, use the following command:

```
awplus# show ipv6 ospf database intra-prefix adv-router  
10.10.10.1
```

Output Figure 23-8: Example output from the **show ipv6 ospf database intra-prefix** command

```
LS age: 1087  
LS Type: AS-External-LSA  
Link State ID: 0.0.0.13  
Advertising Router: 0.0.1.1  
LS Seq Number: 0x8000000C  
Checksum: 0xCE9D  
Length: 52  
Metric Type: 2 (Larger than any link state path)  
Metric: 20  
Prefix: 2010:2222::/64  
Prefix Options: 0 (-|-|-|-)  
Forwarding Address: 2003:1111::1  
...
```

show ipv6 ospf database link

Overview Use this command in User Exec or Privileged Exec modes to display information about the link LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf database link <adv-router-id>
[self-originate|adv-router <adv-router-id>]`

Parameter	Description
<adv-router-id>	The Advertising Router ID (usually entered in IPv4 address format A.B.C.D). Note that this ID component no longer represents an address; it is simply a character string that has an IPv4 address format.
adv-router	Displays all the LSAs of the specified router.
self-originate	Self-originated link states.

Mode User Exec and Privileged Exec

Examples To display information about the link LSAs, use the following command:

```
awplus# show ipv6 ospf database link adv-router 10.10.10.1
```

Output Figure 23-9: Example output from the **show ipv6 ospf database link** command

```
LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.13
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xCE9D
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
...
```

show ipv6 ospf database network

Overview Use this command in User Exec or Privileged Exec modes to display information about the network LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf database network <adv-router-id>
[self-originate|adv-router <adv-router-id>]`

Parameter	Description
<adv-router-id>	The router ID of the advertising router, in IPv4 address format. Note, however, that this no longer represents a real address.
self-originate	Self-originated link states.
adv-router	The advertising router selected.

Mode User Exec and Privileged Exec

Examples To display information about the OSPFv3 network LSAs, use the following command:

```
awplus# show ipv6 ospf database network
```

Output Figure 23-10: Example output from the **show ipv6 ospf database network** command

```
OSPFv3 Router with ID (0.0.1.1) (Process P10)

      Network-LSA (Area 0.0.0.0)

LS age: 97
LS Type: Network-LSA
Link State ID: 0.0.0.202
Advertising Router: 0.0.1.2
LS Seq Number: 0x800000C3
Checksum: 0x92C4
Length: 32
Options: 0x000013 (-|R|-|-|E|V6)
  Attached Router: 0.0.1.2
  Attached Router: 0.0.1.1
```

```
LS age: 1144
LS Type: Network-LSA
Link State ID: 0.0.0.203
Advertising Router: 0.0.1.3
LS Seq Number: 0x800000C4
Checksum: 0x8AC8
Length: 32
Options: 0x000013 (-|R|-|-|E|V6)
  Attached Router: 0.0.1.3
  Attached Router: 0.0.1.1
```

show ipv6 ospf database router

Overview Use this command in User Exec or Privileged Exec modes to display information only about the router LSAs.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf database router <adv-router-id>
[self-originate|adv-router <adv-router-id>]`

Parameter	Description
<adv-router-id>	The router ID of the advertising router, in IPv4 address format. Note, however, that this no longer represents a real address.
self-originate	Self-originated link states.
adv-router	The advertising router selected.

Mode User Exec and Privileged Exec

Examples To display information about the OSPFv3 router LSAs, use the following command:

```
awplus# show ipv6 ospf database router
```

Output Figure 23-11: Example output from the **show ipv6 ospf database router** command

```
OSPFv3 Router with ID (0.0.1.3) (Process P10)

      Router-LSA (Area 0.0.0.0)

LS age: 556
LS Type: Router-LSA
Link State ID: 0.0.0.0
Advertising Router: 0.0.1.1
LS Seq Number: 0x800000CA
Checksum: 0xAA23
Length: 56
Flags: 0x02 (-|-|E|-)
Options: 0x000013 (-|R|-|-|E|V6)
```



```
Link connected to: a Transit Network
Metric: 1
Interface ID: 203
Neighbor Interface ID: 203
Neighbor Router ID: 0.0.1.3

Link connected to: a Transit Network
Metric: 1
Interface ID: 202
Neighbor Interface ID: 202
Neighbor Router ID: 0.0.1.2

LS age: 520
LS Type: Router-LSA
Link State ID: 0.0.0.0
Advertising Router: 0.0.1.2
LS Seq Number: 0x800000D5
Checksum: 0xB328
Length: 40
Flags: 0x00 (-|-|-|-)
Options: 0x000013 (-|R|-|-|E|V6)

Link connected to: a Transit Network
Metric: 1
Interface ID: 202
Neighbor Interface ID: 202
Neighbor Router ID: 0.0.1.2

LS age: 543
LS Type: Router-LSA
Link State ID: 0.0.0.0
Advertising Router: 0.0.1.3
LS Seq Number: 0x800000CC
Checksum: 0xF5EA
Length: 40
Flags: 0x00 (-|-|-|-)
Options: 0x000013 (-|R|-|-|E|V6)

Link connected to: a Transit Network
Metric: 1
Interface ID: 203
Neighbor Interface ID: 203
Neighbor Router ID: 0.0.1.3
OSPFv3 Router with ID (0.0.1.3) (Process P10)

AS-external-LSA
```

```
LS age: 1384
LS Type: AS-External-LSA
Link State ID: 0.0.0.13
Advertising Router: 0.0.1.1
LS Seq Number: 0x80000009
Checksum: 0xD49A
Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1384
LS Type: AS-External-LSA
Link State ID: 0.0.0.14
Advertising Router: 0.0.1.1
LS Seq Number: 0x80000009
Checksum: 0xD696
Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2011:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1384
LS Type: AS-External-LSA
Link State ID: 0.0.0.15
Advertising Router: 0.0.1.1
LS Seq Number: 0x80000009
Checksum: 0xD892
Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2012:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1087
LS Type: AS-External-LSA
Link State ID: 0.0.0.13
Advertising Router: 0.0.1.1
LS Seq Number: 0x8000000C
Checksum: 0xCE9D
Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2010:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
```

```
LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.14
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xD099
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2011:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.15
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xD295
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2012:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.16
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xD491
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2013:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1

LS age: 1087
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.17
  Advertising Router: 0.0.1.1
  LS Seq Number: 0x8000000C
  Checksum: 0xD68D
  Length: 52
    Metric Type: 2 (Larger than any link state path)
    Metric: 20
    Prefix: 2014:2222::/64
    Prefix Options: 0 (-|-|-|-)
    Forwarding Address: 2003:1111::1
```

```
LS age: 1087
LS Type: AS-External-LSA
Link State ID: 0.0.0.18
Advertising Router: 0.0.1.1
LS Seq Number: 0x8000000C
Checksum: 0xD889
Length: 52
  Metric Type: 2 (Larger than any link state path)
  Metric: 20
  Prefix: 2015:2222::/64
  Prefix Options: 0 (-|-|-|-)
  Forwarding Address: 2003:1111::1
```

show ipv6 ospf interface

Overview Use this command in User Exec or Privileged Exec modes to display interface information for OSPF for all interfaces or a specified interface, including OSPFv3 Authentication status for all interfaces or for a specified interface.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf interface [<interface-name>]`

Parameter	Description
<interface-name>	An alphanumeric string that is the interface name. Omit the optional interface to display information for all interfaces.

Mode User Exec and Privileged Exec

Examples `awplus# show ipv6 ospf interface`

Output Figure 23-12: Example output from the **show ipv6 ospf interface** command showing OSPFv3 Authentication configuration information highlighted in bold

```
awplus#show ipv6 ospf interface
eth1 is up, line protocol is up
Interface ID 302
IPv6 Prefixes
  fe80::215:77ff:fead:f87e/64 (Link-Local Address)
Security Policy
  MD5 Authentication SPI 1000
  NULL Encryption SHA-1 Auth, SPI 1001

OSPFv3 Process (10), Area 0.0.0.0, Instance ID 0
Router ID 192.168.1.2, Network Type BROADCAST, Cost: 1
Transmit Delay is 1 sec, State Backup, Priority 1
Interface state Backup
Designated Router (ID) 192.168.1.1
  Interface Address fe80::21d:e5ff:fec9:cfbe
Backup Designated Router (ID) 192.168.1.2
  Interface Address fe80::215:77ff:fead:f87e
Timer interval configured, Hello 10, Dead 40, Wait 40,
Retransmit 5
  Hello due in 00:00:07
Neighbor Count is 1, Adjacent neighbor count is 1
```

Related commands [ipv6 ospf authentication spi](#)
[ipv6 ospf encryption spi esp](#)

show ipv6 ospf neighbor

Overview Use this command in User Exec or Privileged Exec modes to display information on OSPF neighbors. Include the process ID parameter with this command to display information about specified processes.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf [<process-id>] neighbor <neighbor-id>`
`show ipv6 ospf [<process-id>] neighbor detail`
`show ipv6 ospf [<process-id>] neighbor <interface> [detail]`

Parameter	Description
<process-id>	<character string> The ID of the OSPF process for which information will be displayed.
<neighbor-id>	The Neighbor ID, entered in IP address (A.B.C.D) format.
detail	Detail of all neighbors.
<interface>	IP address of the interface.

Mode User Exec and Privileged Exec

Examples `awplus# show ipv6 ospf neighbor`

Output Figure 23-13: Example output from **show ipv6 ospf neighbor**

```
awplus#show ipv6 ospf P1 neighbor 2.2.2.2
OSPFv3 Process (P1)
Neighbor ID    Pri      State                Dead Time   Interface Instance ID
2.2.2.2        5        2-Way/DROther        00:00:33   eth1           0
```

Figure 23-14: Example output from **show ipv6 ospf neighbor detail**

```
awplus#show ipv6 ospf neighbor detail
Neighbor 0.0.1.2, interface address fe80::215:77ff:fec9:7472
  In the area 0.0.0.0 via interface eth1
  Neighbor priority is 1, State is Full, 6 state changes
  DR is 0.0.1.2      BDR is 0.0.1.1
  Options is 0x000013 (-|R|-|-|E|V6)
  Dead timer due in 00:00:33
  Database Summary List 0
  Link State Request List 0
  Link State Retransmission List 0
```

show ipv6 ospf route

Overview Use this command in User Exec or Privileged Exec modes to display the OSPF routing table. Include the process ID parameter with this command to display the OSPF routing table for specified processes.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf [<process-id>] route`

Parameter	Description
<code><process-id></code>	A character string that specifies the router process. If this parameter is included, only the information for this specified routing process is displayed.

Mode User Exec and Privileged Exec

Examples To display the whole OSPF routing table, use the command:

```
awplus# show ipv6 ospf route
```

Output Figure 23-15: Example output from the **show ipv6 ospf P1 route** command for a specific process

```
OSPFv3 Process (P1)
Codes: C - connected, D - Discard, O - OSPF, IA - OSPF inter area
E1 - OSPF external type 1, E2 - OSPF external type 2

Destination Metric
Next-hop
O  2002:1111::/64  2
via fe80::200:cdff:fe24:daae, eth1, Area 0.0.0.0
...
```

show ipv6 ospf virtual-links

Overview Use this command in User Exec or Privileged Exec modes to display virtual link information, including OSPFv3 Authentication status for virtual links.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Syntax `show ipv6 ospf virtual-links`

Mode User Exec and Privileged Exec

Usage notes See the [OSPFv3 Feature Overview and Configuration Guide](#) for more information and examples.

Examples To display virtual link information, use the command:

```
awplus# show ipv6 ospf virtual-links
```

Output Figure 23-16: Example output from the **show ipv6 ospf virtual-links** command showing OSPFv3 Authentication configuration information highlighted in bold

```
awplus#show ipv6 ospf virtual-links
Virtual Link VLINK1 to router 192.168.1.10 is down
  Transit area 0.0.0.1 via interface *, instance ID 0
  Local address
  Remote address
MD5 Authentication SPI 1000
NULL encryption SHA-1 auth SPI 1001
  Transmit Delay is 1 sec, State Down,
  Timer intervals configured, Hello 10, Dead 40, Wait 40,
  Retransmit 5
    Hello due in inactive
    Adjacency state Down
```

Related commands [area virtual-link authentication ipsec spi](#)
[area virtual-link encryption ipsec spi](#)

summary-address (IPv6 OSPF)

Overview Use this command in Router Configuration mode to summarize, or possibly suppress, external redistributed OSPFv3 routes within the specified address range.

Use the **no** variant of this command in Router Configuration mode to stop summarizing, or suppressing, external redistributed OSPFv3 routes within the specified address range.

Syntax `summary-address <ipv6-addr/prefix-length> [not-advertise] [tag <0-4294967295>]`
`no summary-address <ipv6-addr/prefix-length> [not-advertise] [tag <0-4294967295>]`

Parameter	Description
<code><ipv6-addr/prefix-length></code>	Specifies the base IPv6 address of the IPv6 summary address. The range of addresses given as IPv6 starting address and an IPv6 prefix length.
<code>not-advertise</code>	Set the not-advertise option if you do not want OSPFv3 to advertise either the summary address or the individual networks within the range of the summary address.
<code>tag <0-4294967295></code>	The tag parameter specifies the tag value that OSPFv3 places in the AS external LSAs created as a result of redistributing the summary route. The tag overrides tags set by the original route.

Default The default tag value for a summary address is 0.

Mode Router Configuration

Usage An address range is a pairing of an address and a prefix length. Redistributing routes from other protocols into OSPFv3 requires the router to advertise each route individually in an external LSA. Use this command to advertise one summary route for all redistributed routes covered by a specified prefix to decrease the size of the OSPFv3 link state database.

For example, if the specified address range is 2001:0db8:44::/48, then summary-address functionality will match 2001:0db8:4400:0000::1/128 through 2001:0db8:44ff:ffff::1/128.

Ensure OSPFv3 routes exist in the summary address range for advertisement before using this command.

Example The following example uses the `summary-address` command to aggregate external LSAs that match the IPv6 prefix `2001:0db8::/32` and assigns a tag value of 3.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# summary-address 2001:0db8::/32 tag 3
```

The following example uses the `no summary-address` command to stop summarizing IPv6 addresses in the address range covered within the IPv6 prefix `2001:0db8::/32`.

```
awplus# configure terminal
awplus(config)# router ipv6 ospf
awplus(config-router)# no summary-address 2001:0db8::/32
```

timers spf exp (IPv6 OSPF)

Overview Use this command to adjust route calculation timers using exponential back-off delays.

Use **no** form of this command to return to the default exponential back-off timer values.

Syntax `timers spf exp <min-holdtime> <max-holdtime>`
`no timers spf exp <min-holdtime> <max-holdtime>`

Parameter	Description
<code><min-holdtime></code>	Specifies the minimum delay between receiving a change to the SPF calculation in milliseconds. The range is 0-2147483647. The default SPF min-holdtime value is 50 milliseconds.
<code><max-holdtime></code>	Specifies the maximum delay between receiving a change to the SPF calculation in milliseconds. The range is 0-2147483647. The default SPF max-holdtime value is 50 seconds.

Mode Router Configuration

Usage notes This command configures the minimum and maximum delay time between the receipt of a topology change and the calculation of the Shortest Path First (SPF).
The time between SPF runs increases if a topology change occurs (and triggers a new SPF run) before the last SPF holdtimer has finished. The time between runs may increase up to the max-holdtime value. This increase in holdtime prevents too many SPF runs from occurring if multiple OSPF topology change events occur.

Examples To set the minimum delay time to 5 milliseconds and maximum delay time to 2 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 ospf 100
awplus(config-router)# timers spf exp 5 2000
```

Related commands [show ipv6 ospf](#)

undebbug ipv6 ospf events

Overview This command applies the functionality of the no [debug ipv6 ospf events](#) command.

undebbug ipv6 ospf ifsm

Overview This command applies the functionality of the no `debug ipv6 ospf ifsm` command.

undebbug ipv6 ospf lsa

Overview This command applies the functionality of the no `debug ipv6 ospf lsa` command.

undebg ipv6 ospf nfsm

Overview This command applies the functionality of the no [debug ipv6 ospf nfsm](#) command.

undebg ipv6 ospf packet

Overview This command applies the functionality of the no `debug ipv6 ospf packet` command.

undebbug ipv6 ospf route

Overview This command applies the functionality of the no [debug ipv6 ospf route](#) command.

24

BGP and BGP4+ Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure the Border Gateway Protocol for IPv4 (BGP) and for IPv6 (BGP4+).

For basic BGP and BGP4+ introduction information and configuration examples, see the [Routing_Protocol Guide](#).

- Command List**
- “[address-family](#)” on page 924
 - “[aggregate-address](#)” on page 926
 - “[auto-summary \(BGP only\)](#)” on page 929
 - “[bgp aggregate-nexthop-check](#)” on page 931
 - “[bgp always-compare-med](#)” on page 932
 - “[bgp bestpath as-path ignore](#)” on page 934
 - “[bgp bestpath compare-confed-aspath](#)” on page 935
 - “[bgp bestpath compare-routerid](#)” on page 936
 - “[bgp bestpath med](#)” on page 937
 - “[bgp bestpath med remove-recv-med](#)” on page 939
 - “[bgp bestpath med remove-send-med](#)” on page 940
 - “[bgp client-to-client reflection](#)” on page 941
 - “[bgp cluster-id](#)” on page 942
 - “[bgp confederation identifier](#)” on page 944
 - “[bgp confederation peers](#)” on page 945
 - “[bgp config-type](#)” on page 947
 - “[bgp dampening](#)” on page 949
 - “[bgp damp-peer-oscillation \(BGP only\)](#)” on page 951

- “[bgp default ipv4-unicast](#)” on page 952
- “[bgp default local-preference \(BGP only\)](#)” on page 953
- “[bgp deterministic-med](#)” on page 954
- “[bgp enforce-first-as](#)” on page 956
- “[bgp fast-external-failover](#)” on page 957
- “[bgp graceful-restart](#)” on page 958
- “[bgp graceful-restart graceful-reset](#)” on page 960
- “[bgp log-neighbor-changes](#)” on page 961
- “[bgp memory maxallocation](#)” on page 963
- “[bgp nexthop-trigger-count](#)” on page 964
- “[bgp nexthop-trigger delay](#)” on page 965
- “[bgp nexthop-trigger enable](#)” on page 966
- “[bgp rfc1771-path-select \(BGP only\)](#)” on page 967
- “[bgp rfc1771-strict \(BGP only\)](#)” on page 968
- “[bgp router-id](#)” on page 969
- “[bgp scan-time \(BGP only\)](#)” on page 971
- “[bgp update-delay](#)” on page 972
- “[clear bgp *](#)” on page 973
- “[clear bgp \(IPv4 or IPv6 address\)](#)” on page 974
- “[clear bgp \(ASN\)](#)” on page 976
- “[clear bgp external](#)” on page 977
- “[clear bgp peer-group](#)” on page 978
- “[clear bgp ipv6 \(ipv6 address\) \(BGP4+ only\)](#)” on page 979
- “[clear bgp ipv6 dampening \(BGP4+ only\)](#)” on page 980
- “[clear bgp ipv6 flap-statistics \(BGP4+ only\)](#)” on page 981
- “[clear bgp ipv6 \(ASN\) \(BGP4+ only\)](#)” on page 982
- “[clear bgp ipv6 external \(BGP4+ only\)](#)” on page 983
- “[clear bgp ipv6 peer-group \(BGP4+ only\)](#)” on page 984
- “[clear ip bgp * \(BGP only\)](#)” on page 985
- “[clear ip bgp \(IPv4\) \(BGP only\)](#)” on page 986
- “[clear ip bgp dampening \(BGP only\)](#)” on page 987
- “[clear ip bgp flap-statistics \(BGP only\)](#)” on page 988
- “[clear ip bgp \(ASN\) \(BGP only\)](#)” on page 989
- “[clear ip bgp external \(BGP only\)](#)” on page 990
- “[clear ip bgp peer-group \(BGP only\)](#)” on page 991

- [“clear ip prefix-list”](#) on page 992
- [“debug bgp \(BGP only\)”](#) on page 993
- [“distance \(BGP and BGP4+\)”](#) on page 995
- [“exit-address-family”](#) on page 997
- [“ip community-list”](#) on page 998
- [“ip community-list expanded”](#) on page 1000
- [“ip community-list standard”](#) on page 1002
- [“ip extcommunity-list expanded”](#) on page 1004
- [“ip extcommunity-list standard”](#) on page 1006
- [“ip prefix-list”](#) on page 1008
- [“ipv6 prefix-list”](#) on page 1010
- [“match as-path”](#) on page 1012
- [“match community”](#) on page 1013
- [“max-paths”](#) on page 1015
- [“neighbor activate”](#) on page 1016
- [“neighbor advertisement-interval”](#) on page 1019
- [“neighbor allowas-in”](#) on page 1022
- [“neighbor as-origination-interval”](#) on page 1025
- [“neighbor attribute-unchanged”](#) on page 1027
- [“neighbor capability graceful-restart”](#) on page 1030
- [“neighbor capability orf prefix-list”](#) on page 1033
- [“neighbor capability route-refresh”](#) on page 1036
- [“neighbor collide-established”](#) on page 1039
- [“neighbor default-originate”](#) on page 1042
- [“neighbor description”](#) on page 1045
- [“neighbor disallow-infinite-holdtime”](#) on page 1048
- [“neighbor dont-capability-negotiate”](#) on page 1050
- [“neighbor ebgp-multihop”](#) on page 1053
- [“neighbor enforce-multihop”](#) on page 1056
- [“neighbor filter-list”](#) on page 1059
- [“neighbor interface”](#) on page 1062
- [“neighbor local-as”](#) on page 1064
- [“neighbor maximum-prefix”](#) on page 1067
- [“neighbor next-hop-self”](#) on page 1070
- [“neighbor override-capability”](#) on page 1073

- [“neighbor passive”](#) on page 1075
- [“neighbor password”](#) on page 1078
- [“neighbor peer-group \(add a neighbor\)”](#) on page 1081
- [“neighbor peer-group \(create a peer-group\)”](#) on page 1083
- [“neighbor port”](#) on page 1084
- [“neighbor prefix-list”](#) on page 1087
- [“neighbor remote-as”](#) on page 1090
- [“neighbor remove-private-AS \(BGP only\)”](#) on page 1093
- [“neighbor restart-time”](#) on page 1095
- [“neighbor route-map”](#) on page 1098
- [“neighbor route-reflector-client \(BGP only\)”](#) on page 1102
- [“neighbor route-server-client \(BGP only\)”](#) on page 1104
- [“neighbor send-community”](#) on page 1105
- [“neighbor shutdown”](#) on page 1109
- [“neighbor soft-reconfiguration inbound”](#) on page 1111
- [“neighbor timers”](#) on page 1114
- [“neighbor transparent-as”](#) on page 1117
- [“neighbor transparent-nexthop”](#) on page 1119
- [“neighbor unsuppress-map”](#) on page 1121
- [“neighbor update-source”](#) on page 1124
- [“neighbor version \(BGP only\)”](#) on page 1128
- [“neighbor weight”](#) on page 1130
- [“network \(BGP and BGP4+\)”](#) on page 1133
- [“network synchronization”](#) on page 1136
- [“redistribute \(into BGP or BGP4+\)”](#) on page 1137
- [“restart bgp graceful \(BGP only\)”](#) on page 1139
- [“router bgp”](#) on page 1140
- [“route-map”](#) on page 1141
- [“set as-path”](#) on page 1144
- [“set community”](#) on page 1145
- [“show bgp ipv6 \(BGP4+ only\)”](#) on page 1147
- [“show bgp ipv6 community \(BGP4+ only\)”](#) on page 1148
- [“show bgp ipv6 community-list \(BGP4+ only\)”](#) on page 1150
- [“show bgp ipv6 dampening \(BGP4+ only\)”](#) on page 1151
- [“show bgp ipv6 filter-list \(BGP4+ only\)”](#) on page 1152

- [“show bgp ipv6 inconsistent-as \(BGP4+ only\)”](#) on page 1153
- [“show bgp ipv6 longer-prefixes \(BGP4+ only\)”](#) on page 1154
- [“show bgp ipv6 neighbors \(BGP4+ only\)”](#) on page 1155
- [“show bgp ipv6 paths \(BGP4+ only\)”](#) on page 1158
- [“show bgp ipv6 prefix-list \(BGP4+ only\)”](#) on page 1159
- [“show bgp ipv6 quote-regexp \(BGP4+ only\)”](#) on page 1160
- [“show bgp ipv6 regexp \(BGP4+ only\)”](#) on page 1161
- [“show bgp ipv6 route-map \(BGP4+ only\)”](#) on page 1163
- [“show bgp ipv6 summary \(BGP4+ only\)”](#) on page 1164
- [“show bgp memory maxallocation \(BGP only\)”](#) on page 1165
- [“show bgp nexthop-tracking \(BGP only\)”](#) on page 1166
- [“show bgp nexthop-tree-details \(BGP only\)”](#) on page 1167
- [“show debugging bgp \(BGP only\)”](#) on page 1168
- [“show ip bgp \(BGP only\)”](#) on page 1169
- [“show ip bgp attribute-info \(BGP only\)”](#) on page 1170
- [“show ip bgp cidr-only \(BGP only\)”](#) on page 1171
- [“show ip bgp community \(BGP only\)”](#) on page 1172
- [“show ip bgp community-info \(BGP only\)”](#) on page 1174
- [“show ip bgp community-list \(BGP only\)”](#) on page 1175
- [“show ip bgp dampening \(BGP only\)”](#) on page 1176
- [“show ip bgp filter-list \(BGP only\)”](#) on page 1178
- [“show ip bgp inconsistent-as \(BGP only\)”](#) on page 1179
- [“show ip bgp longer-prefixes \(BGP only\)”](#) on page 1180
- [“show ip bgp neighbors \(BGP only\)”](#) on page 1181
- [“show ip bgp neighbors connection-retrytime \(BGP only\)”](#) on page 1184
- [“show ip bgp neighbors hold-time \(BGP only\)”](#) on page 1185
- [“show ip bgp neighbors keepalive \(BGP only\)”](#) on page 1186
- [“show ip bgp neighbors keepalive-interval \(BGP only\)”](#) on page 1187
- [“show ip bgp neighbors notification \(BGP only\)”](#) on page 1188
- [“show ip bgp neighbors open \(BGP only\)”](#) on page 1189
- [“show ip bgp neighbors rcvd-msgs \(BGP only\)”](#) on page 1190
- [“show ip bgp neighbors sent-msgs \(BGP only\)”](#) on page 1191
- [“show ip bgp neighbors update \(BGP only\)”](#) on page 1192
- [“show ip bgp paths \(BGP only\)”](#) on page 1193
- [“show ip bgp prefix-list \(BGP only\)”](#) on page 1194

- [“show ip bgp quote-regexp \(BGP only\)”](#) on page 1195
- [“show ip bgp regexp \(BGP only\)”](#) on page 1197
- [“show ip bgp route-map \(BGP only\)”](#) on page 1199
- [“show ip bgp scan \(BGP only\)”](#) on page 1200
- [“show ip bgp summary \(BGP only\)”](#) on page 1201
- [“show ip community-list”](#) on page 1202
- [“show ip extcommunity-list”](#) on page 1203
- [“show ip prefix-list”](#) on page 1204
- [“show ipv6 prefix-list”](#) on page 1205
- [“show ip protocols bgp \(BGP only\)”](#) on page 1206
- [“show route-map”](#) on page 1207
- [“synchronization”](#) on page 1208
- [“timers \(BGP\)”](#) on page 1210
- [“undebg bgp \(BGP only\)”](#) on page 1212

address-family

Overview This command enters the IPv4 or IPv6 Address-Family Configuration command mode. In this mode you can configure address-family specific parameters.

Syntax [BGP] address-family ipv4 [unicast]
no address-family ipv4 [unicast]

Syntax [BGP4+] address-family ipv6 [unicast]
no address-family ipv6 [unicast]

Parameter	Description
ipv4	Configure parameters relating to the exchange of IPv4 prefixes.
ipv6	Configure parameters relating to the exchange of IPv6 prefixes.
unicast	Configure parameters relating to the exchange of routes to unicast destinations.

Mode [BGP] Router Configuration

Mode [BGP4+] Router Configuration

Usage notes To leave the IPv4 or IPv6 Address Family Configuration mode, and return to the Router Configuration mode, use the [exit-address-family](#) command.

Example [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# neighbor 192.168.0.1 remote-as 100
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 192.168.0.1 activate
awplus(config-router-af)# exit-address-family
awplus(config-router)#
```

Example [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1 activate
awplus(config-router-af)# exit-address-family
awplus(config-router)#
```

Related commands [exit-address-family](#)

**Command
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

aggregate-address

Overview This command adds an aggregate route that can be advertised to BGP or BGP4+ neighbors. This command creates an aggregate entry in the BGP or BGP4+ routing table if the device learns, by any means, any routes that are within the range configured by the aggregate address/mask.

When this command is used with the **summary-only** option, the more-specific routes of the aggregate are suppressed to all neighbors. Use the [neighbor unsuppress-map](#) command instead to selectively leak more-specific routes to a particular neighbor.

The **no** variant of this command removes the aggregate configured by the **aggregate-address** command.

Syntax [BGP] `aggregate-address <ip-addr/m> {summary-only|as-set}`
`no aggregate-address <ip-addr/m> {summary-only|as-set}`

Syntax [BGP4+] `aggregate-address <ipv6-addr/prefix-length>`
`{summary-only|as-set}`
`no aggregate-address <ipv6-addr/prefix-length>`
`{summary-only|as-set}`

Parameter	Description
<code><ip-addr/m></code>	Specifies the aggregate IPv4 address and mask.
<code><ipv6-addr/prefix-length></code>	Specifies the aggregate IPv6 address. The IPv6 address uses the format X:X::X/X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<code>summary-only</code>	Filters more specific routes from updates. Only the aggregate address/mask will be advertised, and none of the component addresses that fall within the range of the aggregate address/mask.
<code>as-set</code>	Generates AS set path information. The AS-path advertised with the aggregate is an unordered list of all the AS-numbers that appear in any of the AS-paths of the component routes, with each AS-number appearing just once in the list.

Mode [BGP] Router Configuration or IPv4 Address Family Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage [BGP] If the `summary-only` parameter is specified, then only the aggregate address/mask will be advertised, and none of the component addresses that fall within the range of the aggregate address/mask. For example, if you configure:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# aggregate-address 172.0.0.0/8 summary-only
```

then the device will advertise the prefix 172.0.0.0/8, but no component routes like 172.10.0.0/16

The `as-set` parameter controls the AS-path attribute that is advertised with the aggregate route. If the device has learned multiple routes that are within the range of the aggregate address/mask, and the AS-paths associated with those routes contain different sets of AS-numbers, then it is not possible to create a single AS-path that accurately represents the AS-paths of all those component routes. In this case, the device will, by default, advertise a NULL AS-path with the aggregate.

Usage [BGP4+] If the `summary-only` parameter is specified, then only the aggregate address/mask will be advertised, and none of the component addresses that fall within the range of the aggregate address/mask. For example, if you configure:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# aggregate-address 2001:0db8::/64
summary-only
```

then the device will advertise the prefix 2001:0db8::/64, but no component routes like 2001:0db8:010d::1/128

Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# aggregate-address 192.0.0.0/8 as-set
summary-only
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no aggregate-address 192.0.0.0/8 as-set
summary-only
```

Examples
[BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address family ipv6
awplus(config-router-af)# aggregate-address 2001:0db8::/64
as-set summary-only

awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address family ipv6
awplus(config-router-af)# no aggregate-address 2001:0db8::/64
as-set summary-only
```

Related commands

- [aggregate-address](#)
- [match as-path](#)

Command changes

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

auto-summary (BGP only)

Overview Use this command to enable sending summarized routes by a BGP speaker to its peers in the Router Configuration mode or in the Address-Family Configuration mode. BGP uses auto-summary to advertise summarized routes.

Use the **no** variant of this command to disable BGP auto-summary.

Syntax `auto-summary`
`no auto-summary`

Default The auto-summary function is disabled by default.

Mode Router Configuration and Address Family IPv4 mode

Usage If certain routes have already been advertised, enabling auto-summary results in non- summarized routes being withdrawn and only summarized routes are advertised. Summarized routes are advertised before non-summarized routes are withdrawn from all connected peers.

If certain routes have already been advertised, disabling auto-summary results in summarized routes being withdrawn and only non-summarized routes are advertised. Non-summarized routes are advertised before summarized routes are withdrawn from all connected peers.

Examples The following example enables auto-summary in Router Configuration mode:

```
awplus# configure
awplus(config)# router bgp 100
awplus(config-router)# auto-summary
```

The following example disables auto-summary in Router Configuration mode:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no auto-summary
```

The following example enables auto-summary in Address Family IPv4 mode:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv4
awplus(config-router-af)# auto-summary
```

The following example disables auto-summary in Address Family IPv4 mode:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no auto-summary
```

**Command
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp aggregate-nexthop-check

Overview This command affects the operation of the summary-only option on the aggregate-address command.

This command enables a mode whereby the summary-only option will only suppress the component routes if those component routes all have the same next hop. If the routes have different next hops, then they will continue to be advertised to peers even if the summary-only option is configured. By default this is disabled.

The **no** variant of this command disables this function.

Syntax `bgp aggregate-nexthop-check`
`no bgp aggregate-nexthop-check`

Default Disabled by default.

Mode Global Configuration

Example `awplus# configure terminal`
`awplus(config)# bgp aggregate-nexthop-check`

Command changes Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp always-compare-med

Overview This command enables BGP to compare the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.

Multi Exit Discriminator (MED) is used in best path selection by BGP. MED is compared after BGP attributes weight, local preference, AS-path and origin have been compared and are equal.

By default, MED comparison is done only among routes from the same autonomous system (AS). Use the **bgp always-compare-mode** command to allow comparison of MEDs from different ASs.

A path with a lower MED value is preferred. For example, if the bgp table contains the following entries, and the **bgp always-compare-med** command has been issued to enable this feature:

- Route1: as-path 400, med 300
- Route2: as-path 200, med 200
- Route3: as-path 400, med 250

Route1 is compared to Route2. Route2 is best of the two (lower MED). Next, Route2 is compared to Route3 and Route2 is chosen best path again (lower MED). If **always-compare-med** was disabled, MED is not taken into account when Route1 and Route2 are compared, because of different ASs and MED is compared for only Route1 and Route3. In this case, Route3 would be the best path. The selected route is also affected by the **bgp deterministic-med** command. See the [bgp deterministic-med](#) command for details.

If this command is used to compare MEDs for all paths, it should be configured on every BGP router in the AS.

The **no** variant of this command disallows the comparison.

Syntax `bgp always-compare-med`
`no bgp always-compare-med`

Default By default this feature is disabled.

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp always-compare-med
```

Related commands [bgp bestpath med](#)
[bgp bestpath as-path ignore](#)
[bgp bestpath compare-routerid](#)
[bgp deterministic-med](#)

**Command
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath as-path ignore

Overview This command prevents the router from considering as-path as a factor in the algorithm for choosing a route.

The **no** variant of this command allows the router to consider as-path in choosing a route.

Syntax `bgp bestpath as-path ignore`
`no bgp bestpath as-path ignore`

Mode Router Configuration

Example `awplus# configure terminal`
`awplus(config)# router bgp 100`
`awplus(config-router)# bgp bestpath as-path ignore`

Related commands [bgp always-compare-med](#)
[bgp bestpath med](#)
[bgp bestpath compare-routerid](#)

Command changes Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath compare-confed-aspath

Overview This command specifies that the AS confederation path length must be used, when available, in the BGP best path decision process. It is effective only when [bgp bestpath as-path ignore](#) command has not been specified.

By default, if BGP receives routes with identical eBGP paths from eBGP peers, BGP does not continue to consider any AS confederation path length attributes that may be associated with the routes.

The **no** variant of this command returns the device to the default state, where the device ignores AS confederation path length in the BGP best path selection process.

Syntax `bgp bestpath compare-confed-aspath`
`no bgp bestpath compare-confed-aspath`

Mode Router Configuration

Example

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath compare-confed-aspath
```

Related commands [bgp bestpath as-path ignore](#)

Command changes Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath compare-routerid

Overview By default, when comparing similar routes from peers, BGP does not consider the router ID of neighbors advertising the routes - BGP simply selects the first received route. Use this command to include router ID in the selection process; similar routes are compared and the route with the lowest router ID is selected.

The **no** variant of this command disables this feature, and returns the device to the default state, where the device ignores the router ID in the BGP best path selection process.

Syntax `bgp bestpath compare-routerid`
`no bgp bestpath compare-routerid`

Mode Router Configuration

Example `awplus# configure terminal`
`awplus(config)# router bgp 100`
`awplus(config-router)# bgp bestpath compare-routerid`

Related commands [show ip bgp \(BGP only\)](#)
[show bgp ipv6 neighbors \(BGP4+ only\)](#)

Command changes Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath med

Overview This command controls how the Multi Exit Discriminator (MED) attribute comparison is performed.

Use the **no** variant of this command to prevent BGP from considering the MED attribute when comparing paths.

Syntax `bgp bestpath med {[confed] [missing-as-worst]}`

Parameter	Description
confed	Compares MED among confederation paths.
missing-as-worst	Treats missing MED as the least preferred one.

Mode Router Configuration

Usage The **confed** parameter enables MED comparison among paths learned from confederation peers. The MED attributes are compared only if there is no external AS (Autonomous System), where an external AS is one that is not within the confederation. If there is an external AS in the path, then the MED comparison is not made.

For example, in the following paths the MED value is not compared with Path3 since it is not in the confederation. MED is compared for Path1 and Path2 only.

- Path1 = 32000 32004, med=4
- Path2 = 32001 32004, med=2
- Path3 = 32003 1, med=1

The effect of the **missing-as-worst** parameter is to treat a missing MED attribute in a path as having a value of infinity, making the path without a MED value the least desirable path. If the **missing-as-worst** parameter is not configured, the missing MED attribute is assigned the value of 0, making the path with the missing MED attribute the best path.

Examples

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath med missing-as-worst
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath med confed
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath med confed missing-as-worst
```

Related commands [bgp always-compare-med](#)
[bgp bestpath as-path ignore](#)
[bgp deterministic-med](#)

Command changes Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath med remove-recv-med

Overview This command removes the Multi Exit Discriminator (MED) attribute from the update messages received by the BGP speaker from its peers. However, the local BGP speaker will send MED attributes in the update messages to its peers, unless specified not to by the **bgp bestpath med remove-send-med** command.

Use the **no** variant of this command to disable this feature.

Syntax `bgp bestpath med remove-recv-med`
`no bgp bestpath med remove-recv-med`

Mode Router Configuration

Example To enable the **remove-recv-med** feature on the BGP speaker belonging to the Autonomous System (AS) 100, enter the command:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath med remove-recv-med
```

Related commands [bgp bestpath med remove-send-med](#)

Command changes Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp bestpath med remove-send-med

Overview This command removes the Multi Exit Discriminator (MED) attribute from the update messages sent by the BGP speaker to its peers. However, the local BGP speaker will consider the MED attribute received from other peers during the decision and route selection process, unless specified not to by the **bgp bestpath med remove-recv-med** command.

Use the **no** variant of this command to disable this feature.

Syntax `bgp bestpath med remove-send-med`
`no bgp bestpath med remove-send-med`

Mode Router Configuration

Example To enable the **remove-send-med** feature on the BGP speaker belonging to the Autonomous System (AS) 100, enter the command:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp bestpath med remove-send-med
```

Related commands [bgp bestpath med remove-recv-med](#)

Command changes Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp client-to-client reflection

Overview This command restores route reflection from a BGP route reflector to clients, and is used to configure routers as route reflectors. Route reflectors are used when all Interior Border Gateway Protocol (iBGP) speakers are not fully meshed.

If the clients are fully meshed the route reflector is not required, use the **no** variant of this command to disable the client-to-client route reflection.

When a router is configured as a route reflector, client-to-client reflection is enabled by default.

The **no** variant of this command turns off client-to-client reflection.

Syntax `bgp client-to-client reflection`
`no bgp client-to-client reflection`

Default This command is enabled by default.

Mode Router Configuration

Example `awplus# configure terminal`
`awplus(config)# router bgp 100`
`awplus(config-router)# no bgp client-to-client reflection`

Related commands [bgp cluster-id](#)
[neighbor route-reflector-client \(BGP only\)](#)
[show bgp ipv6 \(BGP4+ only\)](#)
[show ip bgp \(BGP only\)](#)

Command changes Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp cluster-id

Overview This command configures the cluster-id if the BGP cluster has more than one route reflector. A cluster includes one or more route reflectors and their clients. Usually, each cluster is identified by the router-id of its single route reflector. However, to increase redundancy, a cluster may sometimes have more than one route reflector. All router reflectors in such a cluster are then identified by a cluster-id.

The **bgp cluster-id** command is used to configure the 4 byte cluster ID for clusters with more than one route reflector.

The **no** variant of this command removes the cluster ID.

Syntax `bgp cluster-id {<ip-address>|<cluster-id>}`
`no bgp cluster-id`

Parameter	Description
<code><cluster-id></code>	<code><1-4294967295></code> Route Reflector cluster-id as a 32 bit quantity.
<code><ip-address></code>	<code>A.B.C.D</code> Route Reflector Cluster-id in IP address format.

Mode Router Configuration

Usage The following configuration creates `cluster-id 5` including two `route-reflector- clients`.

```
awplus(config)# router bgp 200
awplus(config-router)# neighbor 2.2.2.2 remote-as 200
awplus(config-router)# neighbor 3.3.3.3 remote-as 200
awplus(config-router)# neighbor 3.3.3.3 route-reflector-client
awplus(config-router)# neighbor 5.5.5.5 remote-as 200
awplus(config-router)# neighbor 5.5.5.5 route-reflector-client
awplus(config-router)# neighbor 6.6.6.6 remote-as 200
awplus(config-router)# bgp cluster-id 5
```

Examples To add a **bgp cluster-id**, apply the example commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp cluster-id 10.10.1.1
```

To remove a bgp cluster-id apply the example commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp cluster-id 10.10.1.1
```

**Related
commands**

[bgp client-to-client reflection](#)
[neighbor route-reflector-client \(BGP only\)](#)
[show bgp ipv6 \(BGP4+ only\)](#)
[show ip bgp \(BGP only\)](#)

**Command
changes**

Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp confederation identifier

Overview This command specifies a BGP confederation identifier.
The **no** variant of this command removes all BGP confederation identifiers.

Syntax `bgp confederation identifier <1-4294967295>`
`no bgp confederation identifier`

Parameter	Description
<code><1-4294967295></code>	Set routing domain confederation AS number.

Mode Router Configuration

Examples `awplus# configure terminal`
`awplus(config)# router bgp 100`
`awplus(config-router)# bgp confederation identifier 1`
`awplus# configure terminal`
`awplus(config)# router bgp 100`
`awplus(config-router)# no bgp confederation identifier`

Related commands [bgp confederation peers](#)

Command changes Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp confederation peers

Overview This command configures the Autonomous Systems (AS) that belong to the same confederation as the current device.

A confederation allows an AS to be divided into several sub-ASs. The overall AS is given a confederation identifier. External routers view only the whole confederation as one AS, whose AS number is the confederation identifier. Each sub-AS is fully meshed within itself and is visible internally to the confederation.

Use the **bgp confederation peer** command to define the list of AS numbers of the sub-ASs in the confederation containing the current device.

The **no** variant of this command removes an autonomous system from the confederation.

Syntax `bgp confederation peers <1-4294967295>`
`no bgp confederation peers <1-4294967295>`

Parameter	Description
<1-4294967295>	AS numbers of eBGP peers that are under same confederation but in a different sub-AS.

Mode Router Configuration

Usage notes In the following configuration of **Router 1** the neighbor 172.210.30.2 and 172.210.20.1 have iBGP connection within AS 100. The neighbor 173.213.30.1 has an BGP connection, but it is within AS 200, which is part of the same confederation. The neighbor 6.6.6.6 has an eBGP connection to external AS 500.

In the configuration of **Router 2**, neighbor 5.5.5.4 has an eBGP connection to confederation 300. Router2 does not know about the ASs 100 and 200, it only knows about confederation 300.

Router 1

```
awplus(config)# router bgp 100
awplus(config-router)# bgp confederation identifier 300
awplus(config-router)# bgp confederation peers 200
awplus(config-router)# neighbor 172.210.30.2 remote-as 100
awplus(config-router)# neighbor 172.210.20.1 remote-as 100
awplus(config-router)# neighbor 173.213.30.1 remote-as 200
awplus(config-router)# neighbor 6.6.6.6 remote-as 300
```

Router 2

```
awplus(config)# router bgp 500
awplus(config-router)# neighbor 5.5.5.4 remote-as 300
```

Example `awplus# configure terminal`
 `awplus(config)# router bgp 100`
 `awplus(config-router)# bgp confederation peers 1234`

Related commands [bgp confederation identifier](#)

Command changes Added to AlliedWare Plus prior to 5.4.6-1
 Version 5.4.7-2.1: BGP support added for x510 and x550 series
 Version 5.4.7-2.4: BGP support added for IE300 series

bgp config-type

Overview Use this command to set the BGP configuration type to either **standard** or **enhanced** types. When you configure the **enhanced** type, then BGP and BGP4+ communities are allowed to be sent and received by default. The **enhanced** type is configured by default.

Use the **no** variant of this command to restore the default BGP configuration type (**enhanced**).

Syntax `bgp config-type {standard|enhanced}`
`no bgp config-type`

Parameter	Description
standard	Specifies the industry standard style configuration. After setting the configuration to standard, make sure to use the neighbor send-community command to send out BGP community attributes. The synchronization command is enabled in the Global Configuration mode and is shown in the configuration.
enhanced	Specifies the enhanced style configuration. The enhanced configuration type requires no specific configuration for sending out BGP standard community and extended community attributes. The synchronization command is enabled by default in the Global Configuration mode and is not shown in configuration output.

Default By default, the BGP configuration type is **enhanced**.

Mode Global Configuration

Usage notes Note that the **enhanced** type default configuration may cause issues in some networks if unauthorized BGP peers are advertising BGP communities to adjust routing decisions.

Changing modes requires you to **reload** your device for the change to take effect:

```
awplus(config)#bgp config-type standard
awplus(config)#exit
awplus#reload
reboot system? (y/n): y
```

When your device reloads, it will load with the standard BGP settings commonly used by most vendors. Apply the **standard** type configuration if you have interoperability issues.

Examples To specify the standard BGP configuration type, enter the following commands:

```
awplus# configure terminal
awplus(config)# bgp config-type standard
```

To specify the enhanced BGP configuration type, enter the following commands:

```
awplus# configure terminal  
awplus(config)# bgp config-type enhanced
```

To restore the default BGP configuration type (enhanced), enter the following commands:

```
awplus# configure terminal  
awplus(config)# no bgp config-type
```

Related commands [neighbor send-community](#)
[synchronization](#)

Command changes Added to AlliedWare Plus prior to 5.4.6-1
Version 5.4.7-2.1: BGP support added for x510 and x550 series
Version 5.4.7-2.4: BGP support added for IE300 series

bgp dampening

Overview This command enables BGP and BGP4+ dampening and sets BGP and BGP4+ dampening parameters. BGP4+ dampening is available from the IPv6 Address Family Configuration mode. BGP dampening is available from the Router Configuration mode.

The **no** variant of this command disables BGP dampening or unsets the BGP dampening parameters.

Syntax

```
bgp dampening
no bgp dampening
bgp dampening <reachtime>
no bgp dampening <reachtime>
bgp dampening <reachtime> <reuse> <suppress> <maxsuppress>
<unreachtime>
no bgp dampening <reachtime> <reuse> <suppress> <maxsuppress>
<unreachtime>
bgp dampening route-map <route-map-name>
no bgp dampening route-map <route-map-name>
```

Parameter	Description
<reachtime>	<1-45> Specifies the reachability half-life time in minutes. The time for the penalty to decrease to one-half of its current value. The default is 15 minutes.
<reuse>	<1-20000> Specifies the reuse limit value. When the penalty for a suppressed route decays below the reuse value, the routes become unsuppressed. The default reuse limit is 750
<suppress>	<1-20000> Specifies the suppress limit value. When the penalty for a route exceeds the suppress value, the route is suppressed. The default suppress limit is 2000.
<maxsuppress>	<1-255> Specifies the max-suppress-time. Maximum time that a dampened route is suppressed. The default max-suppress value is 4 times the half-life time (60 minutes).
<unreachtime>	<1-45> Specifies the un-reachability half-life time for penalty, in minutes.
route-map	Route-map to specify criteria for dampening.
<route-map-name>	Specify the name of the route-map.

Mode [BGP] Router Configuration

Mode [BGP4+] IPv6 Address Family Configuration

Usage notes Route dampening minimizes the instability caused by route flapping. A penalty is added for every flap in a flapping route. As soon as the total penalty reaches the **suppress** limit the advertisement of the route is suppressed. This penalty is decayed according to the configured **half time** value. Once the penalty is lower than the **reuse** limit, the route advertisement is un-suppressed.

The dampening information is purged from the router once the penalty becomes less than half of the **reuse** limit.

Example [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# bgp dampening 20 800 2500 80 25
```

Example [BGP4+]

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# address-family ipv6
awplus(config-router-af)# bgp dampening 20 800 2500 80 25
```

Command changes

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

bgp damp-peer-oscillation (BGP only)

- Overview** Use this command to enable BGP peer oscillating connection damping.
- Use the **no** variant of this command to disable BGP peer oscillating connection damping.
- Syntax** `bgp damp-peer-oscillations`
`no bgp damp-peer-oscillations`
- Default** By default, this functionality is enabled and will not appear in the **show running-config** command output.
- Mode** Router Configuration
- Usage** BGP peers in AlliedWare Plus will automatically attempt to form connections with configured neighbors. Due to misconfiguration these connections may fail and continue to fail until such time as the misconfiguration is detected and fixed. During this time, BGP can quickly cycle through the state machine from Idle through the various Connect states, which can result in large numbers of TCP sessions being opened in a short period of time.
- This command instead adds a delay after a peer enters the Idle state before it can progress to the later states. The default delay is 0 second, increasing by 1 second for each unsuccessful connection attempt, to a maximum of 5 seconds. After a successful BGP route update has been received over a connection, the delay will be reset to 0. This command implements the DampPeerOscillations FSM behavior described in section 8.1 of RFC 4271.
- The command is enabled by default. When disabled, peers will transition out of the Idle state immediately. The command applies globally to all currently configured BGP peers and all future peers to be created.
- Example** To disable peer connection damping, use the commands:
- ```
awplus# configure terminal
awplus(config)# router bgp 1
awplus(config-router)# no bgp damp-peer-oscillations
```
- Command changes** Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# bgp default ipv4-unicast

**Overview** This command configures BGP defaults and activates IPv4-unicast for a peer by default. This affects BGP global configuration. By default, BGP exchanges IPv4 prefixes with a peer.

The **no** variant of this command disables this function. The BGP routing process will no longer exchange IPv4 addressing information with BGP neighbor routers. Note that disabling the exchange of IPv4 prefixes will also enable an IPv6 only BGP4+ network.

**Syntax** `bgp default ipv4-unicast`  
`no bgp default ipv4-unicast`

**Default** This is enabled by default.

**Mode** Router Configuration

**Usage** Use the negated form of this command to enable an IPv6 only BGP4+ network.

**Examples** `awplus# configure terminal`  
`awplus(config)# router bgp 100`  
`awplus(config-router)# bgp default ipv4-unicast`  
`awplus# configure terminal`  
`awplus(config)# router bgp 100`  
`awplus(config-router)# no bgp default ipv4-unicast`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# bgp default local-preference (BGP only)

**Overview** This command changes the default local preference value.

The local preference indicates the preferred path when there are multiple paths to the same destination. The path with the higher preference is preferred.

Use this command to define the default local preference value that the device will advertise for the routes it sends. The preference is sent to all routers and access servers in the local autonomous system.

The **no** variant of this command reverts to the default local preference value of 100.

**Syntax** `bgp default local-preference <pref-value>`  
`no bgp default local-preference [<pref-value>]`

| Parameter                       | Description                                                                                                            |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;pref-value&gt;</code> | <code>&lt;0-4294967295&gt;</code> Configure default local preference value. The default local preference value is 100. |

**Default** By default the local-preference value is 100.

**Mode** Router Configuration

**Examples**

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp default local-preference 2345555
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp default local-preference
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# bgp deterministic-med

**Overview** Use this command to allow or disallow the device to compare the Multi Exit Discriminator (MED) variable when choosing among routes advertised by different peers in the same autonomous system (AS).

Use the **bgp deterministic-med** command to enable this feature to allow the comparison of MED variables when choosing among routes advertised by different peers in the same AS.

Use the **no** variant of this command to disable this feature to disallow the comparison of the MED variable when choosing among routes advertised by different peers in the same AS.

**Syntax** `bgp deterministic-med`  
`no bgp deterministic-med`

**Default** Disabled

**Mode** Router Configuration

**Usage** When the **bgp deterministic-med** command is enabled, routes from the same AS are grouped together and ordered according to their MED values, and the best routes of each group are compared.

The main benefit of this is that the choice of best route then does not depend on the order in which the routes happened to be received, which is rather random and arbitrary.

To see how this works, consider the following set of bgp table entries, all for the same route:

```
1: ASPATH 234, MED 120, internal, IGP metric to NEXT_HOP 40
2: ASPATH 389, MED 190, internal, IGP metric to NEXT_HOP 35
3: ASPATH 234, MED 245, external
```

If **bgp deterministic-med** is not enabled, then entry 3 will be chosen, because it is an external route.

But if BGP deterministic-MED is enabled, the entries will be grouped as follows:

```
Group 1: 1: ASPATH 234, MED 120, internal, IGP metric to NEXT_HOP 40
 3: ASPATH 234, MED 245, external
Group 2: 2: ASPATH 389, MED 190, internal, IGP metric to NEXT_HOP 35
```

**NOTE:** Routes from the same AS are grouped together and ordered by MED.

Entry 1 is chosen as the best route from Group 1, since this route has the lowest MED value. Entry 2 has to be the best route in Group 2, since this is the only route in that group. These two group winners are compared against each other, and

Entry 2 is chosen as the best route because Entry 2 has the lower metric to next-hop.

All routers in an AS should have the same setting for BGP deterministic-MED. All routers in an AS should have BGP deterministic-MED enabled with **bgp deterministic-med**, or all routers in an AS should have BGP deterministic-MED disabled with **no bgp-deterministic-med**.

In the example above, the MED values were not considered when comparing the winners of the two groups (the best routes from the different ASs). To use MED in the comparison of routes from different ASs, use the [bgp always-compare-med](#) command.

### Examples

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp deterministic-med
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp deterministic-med
```

### Related commands

[show ip bgp \(BGP only\)](#)  
[show bgp ipv6 neighbors \(BGP4+ only\)](#)  
[show ip bgp neighbors \(BGP only\)](#)

### Command changes

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

## bgp enforce-first-as

**Overview** Use this command to enforce the denying of eBGP updates in which the neighbor's AS number is not the first AS in the AS-path attribute.

Use the **no** variant of this command to disable this feature.

**Syntax** `bgp enforce-first-as`  
`no bgp enforce-first-as`

**Mode** Router Configuration

**Usage** This command specifies that any updates received from an external neighbor that do not have the neighbor's configured Autonomous System (AS) at the beginning of the AS\_PATH in the received update must be denied. Enabling this feature adds to the security of the BGP network by not allowing traffic from unauthorized systems.

**Example** `awplus# configure terminal`  
`awplus(config)# router bgp 100`  
`awplus(config-router)# bgp enforce-first-as`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# bgp fast-external-failover

**Overview** Use this command to reset a BGP session immediately if the interface used for BGP connection goes down.

Use the **no** variant of this command to disable this feature.

**Syntax** `bgp fast-external-failover`  
`no bgp fast-external-failover`

**Default** Enabled

**Mode** Router Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# router bgp 100`  
`awplus(config-router)# bgp fast-external-failover`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# bgp graceful-restart

**Overview** Use this command to enable BGP and BGP4+ graceful-restart capabilities for restart and stalepath times.

Use the **no** variant of this command to restore restart timers to their default settings.

**Syntax** `bgp graceful-restart [restart-time <delay-value>|  
stalepath-time <delay-value>]`  
`no bgp graceful-restart [restart-time|stalepath-time]`

| Parameter      | Description                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------|
| restart-time   | The maximum time needed for neighbors to restart, in seconds.<br>The default restart-time is 120 seconds.                |
| stalepath-time | The maximum time to retain stale paths from restarting neighbors, in seconds. The default stalepath-time is 120 seconds. |
| <delay-value>  | <1-3600> Maximum time in seconds.                                                                                        |

**Default** Graceful restart is disabled by default. If you enable it and do not specify the restart-time and stalepath-time, they default to 120 seconds.

**Mode** Router Configuration

**Usage notes** The **restart-time** parameter is used for setting the maximum time that a graceful-restart neighbor waits to come back up after a restart. This **restart-time** value is applied to neighbors unless you explicitly override it by configuring the corresponding value on the neighbor.

The **stalepath-time** parameter is used to set the maximum time to preserve stale paths from a gracefully restarted neighbor. All stalepaths, unless reinstated by the neighbor after a re-establishment, will be deleted when time, as specified by the **stalepath-time** parameter, expires.

**Examples** To enable graceful restart, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# bgp graceful-restart
```

To disable graceful restart, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no bgp graceful-restart
```

To enable graceful restart and set the restart time to 150 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# bgp graceful-restart restart-time 150
```

To return the restart-time to its default of 120 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no bgp graceful-restart restart-time
```

**Related commands** [bgp graceful-restart graceful-reset](#)  
[restart bgp graceful \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# bgp graceful-restart graceful-reset

**Overview** This command enables BGP and BGP4+ graceful-restart when a configuration change forces a peer restart.

Use the **no** variant of this command to restore the device to its default state.

**Syntax** `bgp graceful-restart graceful-reset`  
`no bgp graceful-restart graceful-reset`

**Default** Disabled

**Mode** Router Configuration

**Usage** The [bgp graceful-restart](#) command must be enabled before this command is enabled. All events that cause BGP peer reset, including all session reset commands, can trigger graceful-restart.

**Example** To enable the graceful-restart graceful-reset feature on the BGP or BGP4+ peer belonging to Autonomous System (AS) 10, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# bgp graceful-restart graceful-reset
```

To disable the graceful-restart graceful-reset feature on the BGP or BGP4+ peer belonging to Autonomous System (AS) 10, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no bgp graceful-restart graceful-reset
```

**Related commands** [bgp graceful-restart](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# bgp log-neighbor-changes

**Overview** Use this command to enable logging of status change messages without turning on **debug bgp** commands.

Use the **no** variant of this command to disable this feature.

**Syntax** `bgp log-neighbor-changes`  
`no bgp log-neighbor-changes`

**Default** Disabled

**Mode** Router Configuration

**Usage notes** AlliedWare Plus™ provides other kinds of logging services for neighbor status, for example, **debug bgp fsm** and **debug bgp events**.

However, these commands create a significant hit in the logging performance. If you need to log neighbor status changes only, we recommend turning off all the debug commands, and then use this command.

To see BGP neighbor changes in the log you must also set the log level to informational using the **log buffered** command.

A sample output of this log is:

```
%Protocol-Severity-Events: Message-text
```

A sample output of the log for an interface down event is:

```
%BGP-5-ADJCHANGE: neighbor 10.10.0.24 Down Interface flap
```

The **bgp log-neighbor-changes** command logs the following events:

- BGP Notification Received
- Erroneous BGP Update Received
- User reset request
- Peer time-out
- Peer Closing down the session
- Interface flap
- Router ID changed
- Neighbor deleted
- Member added to peer group
- Administrative shutdown

- Remote AS changed
- RR client configuration modification
- Soft reconfiguration modification

**Example** To enable the logging of BGP status changes without using the debug bgp command:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp log-neighbor-changes
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# bgp memory maxallocation

**Overview** This command allocates a maximum percentage of the RAM (Random Access Memory) available on the device for BGP processes.

When this percentage is exceeded, BGP peering terminates and an **out of resources** error displays. The default setting for **bgp memory maxallocation** is 100% memory allocation.

Use the **no** variant of this command to reset memory allocation to the default.

**Syntax** `bgp memory maxallocation <1-100>`  
`no bgp memory maxallocation`

| Parameter | Description                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------|
| <1-100>   | Percentage of device memory allocated to BGP processes. Note this is RAM (Random Access Memory), not device flash memory. |

**Default** BGP processes are allocated the maximum percentage of 100% of the device's available RAM memory by default. Note only non-default BGP memory allocation values are shown in the running or startup configuration files:

```
awplus#show running-config
!
bgp memory maxallocation 50
!
```

**Mode** Global Configuration

**Examples** To limit the maximum amount of memory used by BGP processes to 65% of the total RAM memory available on the device, use the commands:

```
awplus# configure terminal
awplus(config)# bgp memory maxallocation 65
```

To return to the default 100% maximum RAM memory allocation available on the device for BGP processes, use the commands:

```
awplus# configure terminal
awplus(config)# no bgp memory maxallocation
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# bgp nexthop-trigger-count

**Overview** Use this command to configure the display of BGP next hop tracking status.  
Use the **no** variant of this command to disable this function.

**Syntax** `bgp nexthop-trigger-count <0-127>`  
`no bgp nexthop-trigger-count`

| Parameter | Description                   |
|-----------|-------------------------------|
| <0-127>   | BGP next hop tracking status. |

**Mode** Router Configuration

**Example** To enable next-hop-tracking status on the BGP peer belonging to the Autonomous System (AS) 100, enter the following commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp nexthop-trigger-count 10
```

To disable next-hop-tracking status, enter the following commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp nexthop-trigger-count
```

**Related commands** [bgp nexthop-trigger delay](#)  
[bgp nexthop-trigger enable](#)  
[show bgp nexthop-tracking \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# bgp nexthop-trigger delay

**Overview** Use this command to set the delay interval for next hop address tracking.  
Use the **no** variant of this command to reset the timer value to the default.

**Syntax** `bgp nexthop-trigger delay <1-100>`  
`no bgp nexthop-trigger delay`

| Parameter | Description                                 |
|-----------|---------------------------------------------|
| <1-100>   | Next hop trigger delay interval in seconds. |

**Default** The default next hop delay interval is 5 seconds.

**Mode** Global Configuration

**Usage** This command configures the delay interval between routing table waits for next hop delay tracking. The delay interval determines how long BGP waits after it receives the trigger from the system about one or more next hop changes before it walks the full BGP table to determine which prefixes are affected by the next hop changes.

**Example** To set the next hop delay interval to 6 seconds, enter the command:

```
awplus# configure terminal
awplus(config)# bgp nexthop-trigger delay 6
```

**Related commands** [bgp nexthop-trigger-count](#)  
[bgp nexthop-trigger enable](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# bgp nexthop-trigger enable

**Overview** Use this command to enable next hop address tracking. If next hop address tracking is enabled and a next hop trigger delay interval has not been explicitly set with the [bgp nexthop-trigger delay](#) command, the default delay interval of 5 seconds is used.

Use the **no** variant of this command to disable this feature.

**Syntax** `bgp nexthop-trigger enable`  
`no bgp nexthop-trigger enable`

**Default** Disabled.

**Mode** Global Configuration

**Usage** Next hop address tracking is an event driven notification system that monitors the status of routes installed in the Routing Information Base (RIB) and reports next hop changes that affect internal BGP (iBGP) or external BGP (eBGP) prefixes directly to the BGP process. This improves the overall BGP convergence time, by allowing BGP to respond rapidly to next hop changes for routes installed in the RIB.

If next hop tracking is enabled after certain routes are learned, the registration of all the next hops of selected BGP routes are done immediately after the next hop tracking feature is enabled.

If next hop tracking is disabled, and if there are still some selected BGP routes, BGP deregisters the next hops of all of the selected BGP routes from the system.

If next hop tracking is disabled when next hop tracking is in the process of execution, an error appears, and next hop tracking is not disabled. However, if the next hop tracking timer is running at the time of negation, the next hop tracking timer is stopped, and next hop tracking is disabled.

**Example** To enable next hop address tracking, enter the command:

```
awplus# configure terminal
awplus(config)# bgp nexthop-trigger enable
```

**Related commands** [bgp nexthop-trigger-count](#)  
[bgp nexthop-trigger delay](#)  
[show bgp nexthop-tracking \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

## bgp rfc1771-path-select (BGP only)

**Overview** Use this command to set the RFC1771 compatible path selection mechanism.

Use the **no** variant of this command to revert this setting.

**Syntax** `bgp rfc1771-path-select`  
`no bgp rfc1771-path-select`

**Default** Industry standard compatible path selection mechanism.

**Mode** Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# bgp rfc1771-path-select`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

## bgp rfc1771-strict (BGP only)

- Overview** Use this command to set the Strict RFC1771 setting.  
Use the **no** variant of this command to revert this setting.
- Syntax** `bgp rfc1771-strict`  
`no bgp rfc1771-strict`
- Default** Disabled
- Mode** Global Configuration
- Example** `awplus# configure terminal`  
`awplus(config)# bgp rfc1771-strict`
- Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# bgp router-id

**Overview** Use this command to configure the router identifier. The IPv4 address specified in this command does not have to be an IPv4 address that is configured on any of the interfaces on the device. Note that you must specify an IPv4 address with this when used for BGP4+.

Use the **no** variant of this command to return the router-id to its default value (as described in Default below).

**Syntax** `bgp router-id <routerid>`  
`no bgp router-id [<routerid>]`

| Parameter  | Description                                                                                       |
|------------|---------------------------------------------------------------------------------------------------|
| <routerid> | Specify the IPv4 address without mask for a manually configured router ID, in the format A.B.C.D. |

**Default** If the BGP router ID is not specified, the IPv4 address of the loopback interface is used. When there is no address on the loopback interface, the highest IP address among the other interfaces is used.

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Usage** Use the **bgp router-id** command to manually configure a fixed router ID as a BGP or BGP4+ router identifier. This router ID takes precedence over all other possible router ID sources. The order of precedence is:

- 1) router ID configured with this command
- 2) IP address of the loopback interface
- 3) highest IP address from the other interfaces

**Examples** To configure a router ID with an IPv4 address for a BGP or BGP4+ router identifier, enter the commands listed below:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# bgp router-id 1.1.2.3
```

To disable the router ID for a BGP or BGP4+ router identifier enter the commands listed below:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no bgp router-id
```

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

## bgp scan-time (BGP only)

**Overview** Use this command to set the interval for BGP route next-hop scanning.  
Use the **no** variant of this command to disable this function.

**Syntax** `bgp scan-time <time>`  
`no bgp scan-time [<time>]`

| Parameter | Description                          |
|-----------|--------------------------------------|
| <time>    | <0-60> Scanning interval in seconds. |

**Default** The default scanning interval is 60 seconds.

**Mode** Router Configuration

**Usage** Use this command to configure scanning intervals of BGP routers. This interval is the period after which router checks the validity of the routes in its database.  
To disable BGP scanning, set the scan time interval to 0 seconds.

**Example** `awplus# configure terminal`  
`awplus(config)# router bgp 100`  
`awplus(config-router)# bgp scan-time 10`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# bgp update-delay

**Overview** Use this command to specify the update-delay value for a graceful-restart capable router.

Use the **no** variant of this command to revert to the default update-delay value.

**Syntax** `bgp update-delay <1-3600>`  
`no bgp update-delay [<1-3600>]`

| Parameter | Description             |
|-----------|-------------------------|
| <1-3600>  | Delay value in seconds. |

**Default** The default update-delay value is 120 seconds.

**Mode** Router Configuration

**Usage** The update-delay value is the maximum time a graceful-restart capable router which is restarting will defer route-selection and advertisements to all its graceful-restart capable neighbors. This maximum time starts from the instance the first neighbor attains established state after restart. The restarting router prematurely terminates this timer when end-of-rib markers are received from all its graceful-restart capable neighbors.

**Example** `awplus# configure terminal`  
`awplus(config)# router bgp 10`  
`awplus(config-router)# bgp update-delay 345`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# clear bgp \*

**Overview** Use this command to reset the BGP and BGP4+ connections for all peers.

**Syntax**

```
clear bgp *
clear bgp * in [prefix-filter]
clear bgp * out
clear bgp * soft [in|out]
```

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| *             | Clears all BGP and BGP4+ peers.                                                                                                                                                                                                                                                                                                       |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples**

```
awplus# clear bgp * soft in
awplus# clear bgp * in prefix-filter
```

**Command changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# clear bgp (IPv4 or IPv6 address)

**Overview** Use this command to reset the BGP and BGP4+ connections for specified peers.

**Syntax [BGP]**

```
clear bgp <ip-addr>
clear bgp <ip-addr> in [prefix-filter]
clear bgp <ip-addr> out
clear bgp <ip-addr> soft [in|out]
```

**Syntax [BGP4+]**

```
clear bgp <ipv6-addr>
clear bgp <ipv6-addr> in [prefix-filter]
clear bgp <ipv6-addr> out
clear bgp <ipv6-addr> soft [in|out]
```

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-addr>     | Specifies the IPv4 address of the neighbor whose connection is to be reset, entered in the form A.B.C.D.                                                                                                                                                                                                                              |
| <ipv6-addr>   | Specifies the IPv6 address of the neighbor whose connection is to be reset, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                            |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples [BGP]**

```
awplus# clear bgp 3.3.3.3 soft in prefix-filter
awplus# clear bgp 2.2.2.2 out
```

**Examples [BGP4+]**

```
awplus# clear bgp 2001:0db8:010d::1 soft in prefix-filter
awplus# clear bgp 2001:0db8:010d::1 out
```

**Related commands** [clear bgp \(IPv4 or IPv6 address\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# clear bgp (ASN)

**Overview** Use this command to reset the BGP and BGP4+ connections for peers in the specified Autonomous System Number (ASN).

**Syntax** `clear bgp <asn> [in [prefix-filter]|out|soft [in|out]]`

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <asn>         | <1-4294967295><br>The AS Number for which all routes will be cleared.                                                                                                                                                                                                                                                                 |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples**

```
awplus# clear bgp 300 soft in prefix-filter
awplus# clear bgp 500 soft out
awplus# clear bgp 300 soft in
awplus# clear bgp 1 in prefix-filter
```

**Command changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# clear bgp external

**Overview** Use this command to reset the BGP and BGP4+ connections for all external peers.

**Syntax** `clear bgp external [in [prefix-filter]|out|soft [in|out]]`

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| external      | Clears all external peers.                                                                                                                                                                                                                                                                                                            |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples** `awplus# clear bgp external soft in`  
`awplus# clear bgp external in prefix-filter`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# clear bgp peer-group

**Overview** Use this command to reset the BGP and BGP4+ connections for all members of a peer group.

**Syntax** `clear bgp peer-group <peer-group> [in [prefix-filter] | out | soft [in | out]]`

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer-group    | Clears all members of a peer group.                                                                                                                                                                                                                                                                                                   |
| <peer-group>  | Name of the BGP peer group                                                                                                                                                                                                                                                                                                            |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples** `awplus# clear bgp peer-group P1 soft in`  
`awplus# clear bgp peer-group P2 in`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# clear bgp ipv6 (ipv6 address) (BGP4+ only)

**Overview** Use this command to reset the IPv6 BGP4+ connection to the peer specified by the IP address.

**Syntax** `clear bgp ipv6 <ipv6-addr> [in [prefix-filter]|out|soft [in|out]]`

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv6-addr>   | Specifies the IPv6 address of the neighbor whose connection is to be reset, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                            |
| ipv6          | Clears all IPv6 address family peers. Configure parameters relating to the BGP4+ exchange of IPv6 prefixes.                                                                                                                                                                                                                           |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples** Use the following command to clear the BGP4+ connection to peer at IPv6 address 2001:0db8:010d::1, and clearing all incoming routes.

```
awplus# clear ip bgp 2001:0db8:010d::1 in
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

## clear bgp ipv6 dampening (BGP4+ only)

**Overview** Use this command to clear route dampening information and unsuppress routes that have been suppressed routes.

**Syntax** `clear bgp ipv6 dampening`  
`[<ipv6-addr>|<ipv6-addr/prefix-length>]`

| Parameter                                    | Description                                                                                                                                                                                          |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-addr&gt;</code>               | Specifies the IPv6 address for which BGP4+ dampening is to be cleared, entered in hexadecimal in the format X:X::X:X.                                                                                |
| <code>&lt;ipv6-addr/prefix-length&gt;</code> | Specifies the IPv6 address and prefix-length for which BGP4+ dampening is to be cleared. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64. |

**Mode** Privileged Exec

**Examples** `awplus# clear bgp ipv6 dampening 2001:0db8:010d::1`  
`awplus# clear bgp ipv6 dampening 2001:0db8::/64`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# clear bgp ipv6 flap-statistics (BGP4+ only)

**Overview** Use this command to clear the flap count and history duration for the specified prefixes.

**Syntax** `clear bgp ipv6 flap-statistics`  
`[<ipv6-addr>|<ipv6-addr/prefix-length>]`

| Parameter                                    | Description                                                                                                                                                                                                                  |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-addr&gt;</code>               | Specifies the IPv6 address for which BGP4+ flap count and history duration are to be cleared, entered in hexadecimal in the format X:X::X:X.                                                                                 |
| <code>&lt;ipv6-addr/prefix-length&gt;</code> | Specifies the IPv6 address with prefix length for which BGP4+ flap count and history duration are to be cleared. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64. |

**Mode** Privileged Exec

**Examples** `awplus# clear bgp ipv6 flap-statistics 2001:0db8:010d::1`  
`awplus# clear bgp ipv6 flap-statistics 2001:0db8::/64`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# clear bgp ipv6 (ASN) (BGP4+ only)

**Overview** Use this command to reset the BGP4+ connections to all peers in a specified Autonomous System Number (ASN).

**Syntax**

```
clear bgp ipv6 <asn> [in [prefix-filter]|out|soft [in|out]]
clear bgp ipv6 <asn>
clear bgp ipv6 <asn> in [prefix-filter]
clear bgp ipv6 <asn> out
clear bgp ipv6 <asn> soft [in|out]
```

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <asn>         | <1-4294967295><br>Specifies the ASN for which all routes will be cleared.                                                                                                                                                                                                                                                             |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples**

```
awplus# clear bgp ipv6 100
awplus# clear bgp ipv6 100 in
awplus# clear bgp ipv6 100 in prefix-filter
awplus# clear bgp ipv6 100 out
awplus# clear bgp ipv6 100 soft out
awplus# clear bgp ipv6 100 soft in
```

**Command changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# clear bgp ipv6 external (BGP4+ only)

**Overview** Use this command to reset the BGP4+ connections to all external peers.

**Syntax**

```
clear bgp ipv6 external [in [prefix-filter]|out|soft [in|out]]
clear bgp ipv6 external
clear bgp ipv6 external in [prefix-filter]
clear bgp ipv6 external out
clear bgp ipv6 external soft [in|out]
```

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| external      | Clears all external peers.                                                                                                                                                                                                                                                                                                            |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples**

```
awplus# clear bgp ipv6 external in
awplus# clear bgp ipv6 external in prefix
awplus# clear bgp ipv6 external out
awplus# clear bgp ipv6 external soft out
awplus# clear bgp ipv6 external soft in
```

**Command changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# clear bgp ipv6 peer-group (BGP4+ only)

**Overview** Use this command to reset the BGP4+ connections to all members of a peer group.

**Syntax**

```
clear bgp ipv6 peer-group <peer-name>
clear bgp ipv6 peer-group <peer-name> in [prefix-filter]
clear bgp ipv6 peer-group <peer-name> out
clear bgp ipv6 peer-group <peer-name> soft [in|out]
```

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer-group    | Clears all members of a peer group.                                                                                                                                                                                                                                                                                                   |
| <peer-name>   | Specifies the name of the peer group for which all members will be cleared.                                                                                                                                                                                                                                                           |
| ipv6          | Clears all IPv6 address family peers. Configure parameters relating to the BGP4+ exchange of IPv6 prefixes.                                                                                                                                                                                                                           |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Example** awplus# clear bgp ipv6 peer-group Peer1 out

**Command changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

## clear ip bgp \* (BGP only)

**Overview** Use this command to reset all BGP connections, either by fully resetting sessions or by performing soft resets.

**Syntax**

```
clear ip bgp *
clear ip bgp * in
clear ip bgp * out
clear ip bgp * soft [in|out]
clear ip bgp * in [prefix-filter]
```

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| *             | Clears all BGP peers.                                                                                                                                                                                                                                                                                                                 |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples** To clear all BGP peers, use the command:

```
awplus# clear ip bgp *
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

## clear ip bgp (IPv4) (BGP only)

**Overview** Use this command to reset the IPv4 BGP connection to the peer specified by the IP address.

**Syntax [BGP]** `clear ip bgp <ipv4-addr> [in [prefix-filter]|out|soft [in|out]]`

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv4-addr>   | Specifies the IPv4 address of the neighbor whose connection is to be reset, entered in the form A.B.C.D.                                                                                                                                                                                                                              |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local switch, without resetting the connection or clearing the entries in the local switch. So, the local switch stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the switch to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode [BGP]** Privileged Exec

**Examples [BGP]** To clear the BGP connection to the peer at IPv4 address 192.168.1.1 and clear all incoming routes, use the following command:

```
awplus# clear ip bgp 192.168.1.1 in
```

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# clear ip bgp dampening (BGP only)

**Overview** Use this command to clear route dampening information and unsuppress routes that have been suppressed.

**Syntax** `clear ip bgp dampening [<ip-address>|<ip-address/m>]`

| Parameter                         | Description                                                                                                                              |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code>   | Specifies the IPv4 address for which BGP dampening is to be cleared, in dotted decimal format.                                           |
| <code>&lt;ip-address/m&gt;</code> | Specifies the IPv4 address with mask for which BGP dampening is to be cleared, entered in the form A.B.C.D/M. Where M is the subnet mask |
| <code>ipv4</code>                 | Clears all IPv4 address family peers. Configure parameters relating to the BGP exchange of IPv4 prefixes.                                |

**Mode** Privileged Exec

**Examples** `awplus# clear ip bgp dampening 10.10.0.121`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

## clear ip bgp flap-statistics (BGP only)

**Overview** Use this command to clear the flap count and history duration for the specified prefixes.

**Syntax** `clear ip bgp flap-statistics [<ip-address>|<ip-address/m>]`

| Parameter                         | Description                                                                                               |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code>   | Specifies the IPv4 address for which BGP flap count and history duration are to be cleared.               |
| <code>&lt;ip-address/m&gt;</code> | Specifies the IPv4 address with mask for which BGP flap count and history duration are to be cleared.     |
| <code>ipv4</code>                 | Clears all IPv4 address family peers. Configure parameters relating to the BGP exchange of IPv4 prefixes. |

**Mode** Privileged Exec

**Examples** `awplus# clear ip bgp flap-statistics 10.10.0.121`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



## clear ip bgp (ASN) (BGP only)

**Overview** Use this command to reset the BGP connections to all peers in a specified Autonomous System Number (ASN).

**Syntax**

```
clear ip bgp <asn> [in [prefix-filter]|out|soft [in|out]]
clear ip bgp <asn> ipv4
clear ip bgp <asn> ipv4 in [prefix-filter]
clear ip bgp <asn> ipv4 out
clear ip bgp <asn> ipv4 soft [in|out]
```

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <asn>         | <1-4294967295><br>Specifies the ASN for which all routes will be cleared.                                                                                                                                                                                                                                                             |
| ipv4          | Clears all IPv4 address family peers. Configure parameters relating to the BGP exchange of IPv4 prefixes.                                                                                                                                                                                                                             |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples** awplus# clear ip bgp 100

**Command changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# clear ip bgp external (BGP only)

**Overview** Use this command to reset the BGP connections to all external peers.

**Syntax**

```
clear ip bgp external [in [prefix-filter]|out|soft [in|out]]
clear ip bgp external
clear ip bgp external in [prefix-filter]
clear ip bgp external out
clear ip bgp external soft [in|out]
```

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| external      | Clears all external peers.                                                                                                                                                                                                                                                                                                            |
| ipv4          | Clears all IPv4 address family peers. Configure parameters relating to the BGP exchange of IPv4 prefixes.                                                                                                                                                                                                                             |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples** awplus# clear ip bgp external out

**Command changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# clear ip bgp peer-group (BGP only)

**Overview** Use this command to reset the BGP connections to all members of a peer group.

**Syntax**

```
clear ip bgp peer-group <peer-name>
clear ip bgp peer-group <peer-name> in [prefix-filter]
clear ip bgp peer-group <peer-name> out
clear ip bgp peer-group <peer-name> soft [in|out]
clear ip bgp peer-group <peer-name> out
clear ip bgp peer-group <peer-name> soft [in|out]
```

| Parameter     | Description                                                                                                                                                                                                                                                                                                                           |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer-group    | Clears all members of a peer group.                                                                                                                                                                                                                                                                                                   |
| <peer-name>   | Specifies the name of the peer group for which all members will be cleared.                                                                                                                                                                                                                                                           |
| ipv4          | Clears all IPv4 address family peers. Configure parameters relating to the BGP exchange of IPv4 prefixes.                                                                                                                                                                                                                             |
| in            | Indicates that incoming advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| prefix-filter | Specifies that a prefix-list will be sent, by the ORF mechanism, to those neighbors with which the ORF capability has been negotiated. The neighbors will be triggered to resend updates, which match the prefix-list filter, to the local router. The local router will then perform a soft reconfiguration.                         |
| out           | Indicates that outgoing advertised routes will be cleared.                                                                                                                                                                                                                                                                            |
| soft in       | Soft inbound reset causes the neighbors to resend all their updates to the local device, without resetting the connection or clearing the entries in the local device. So, the local device stores new updates, and uses them to systematically replace existing table entries. This process can use a considerable amount of memory. |
| soft out      | Soft outbound reset causes the device to simply resend all its updates to the specified neighbor(s), without resetting the connection, or clearing table entries.                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples** awplus# clear ip bgp peer-group Peer1 out

**Command changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# clear ip prefix-list

**Overview** Use this command to reset the hit count to zero in the prefix-list entries.

**Syntax** `clear ip prefix-list [<list-name>] [<ip-address>/<mask>]`

| Parameter           | Description                  |
|---------------------|------------------------------|
| <list-name>         | The name of the prefix-list. |
| <ip-address>/<mask> | The IP prefix and length.    |

**Mode** Privileged Exec

**Example** To clear a prefix-list named List1:

```
awplus# clear ip prefix-list List1
```

# debug bgp (BGP only)

**Overview** Use this command to turn on one or more BGP debug options.  
Use the **no** variant of this command to disable one or more BGP debug options.

**Syntax**

```
debug bgp
[all|dampening|events|filters|fsm|keepalives|nht|nsm|updates
[in|out]]

no debug all bgp

no debug bgp
[all|dampening|events|filters|fsm|keepalives|nht|nsm|updates
[in|out]]
```

| Parameter  | Description                                                   |
|------------|---------------------------------------------------------------|
| all        | Turns on all debugging for BGP.                               |
| dampening  | Specifies debugging for BGP dampening.                        |
| events     | Specifies debugging for BGP events.                           |
| filters    | Specifies debugging for BGP filters.                          |
| fsm        | Specifies debugging for BGP Finite State Machine (FSM).       |
| keepalives | Specifies debugging for BGP keepalives.                       |
| nht        | Specifies debugging for BGP NHT (Next Hop Tracking) messages. |
| nsm        | Specifies debugging for NSM messages.                         |
| updates    | [in out]<br>Specifies debugging for BGP updates.              |
| in         | Inbound updates.                                              |
| out        | Outbound updates.                                             |

**Mode** Privileged Exec and Global Configuration

**Usage** If the command is entered with no parameters, then all debug options are enabled.

**Examples**

```
awplus# debug bgp
awplus# debug bgp events
awplus# debug bgp nht
awplus# debug bgp updates in
```

**Related commands** [show debugging bgp \(BGP only\)](#)  
[undebug bgp \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

## distance (BGP and BGP4+)

**Overview** This command sets the administrative distance for BGP and BGP4+ routes. The device uses this value to select between two or more routes to the same destination from two different routing protocols. Set the administrative distance for BGP routes in the Router Configuration mode, and for BGP4+ routes in IPv6 Address Family Configuration mode.

The route with the smallest administrative distance value is added to the Forwarding Information Base (FIB). For more information, see the [Route Selection Feature Overview and Configuration Guide](#), which is available from the above link at [alliedtelesis.com](#).

The **no** variant of this command sets the administrative distance for the route to the default for the route type.

**Syntax**

```
distance <1-255> <ip-address/m>
distance bgp <ebgp> <ibgp> <local>
no distance <1-255> <ip-address/m>
no distance bgp <ebgp> <ibgp> <local>
```

| Parameter      | Description                                                                                                                                                                                                            |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-255>        | The administrative distance value you are setting for the route.                                                                                                                                                       |
| <ip-address/m> | The IP source prefix that you are changing the administrative distance for, entered in the form A.B.C.D/M. This is an IPv4 address in dotted decimal notation followed by a forward slash, and then the prefix length. |
| <ebgp>         | Specifies the administrative distance of external BGP (eBGP) routes. These are routes learned from a neighbor out of the AS. Specify the distance as a number between 1 and 255.<br>Default: <b>20</b>                 |
| <ibgp>         | Specifies the administrative distance of internal BGP (iBGP) routes. These are routes learned from a neighbor within the same AS. Specify the distance as a number between 1 and 255.<br>Default: <b>200</b>           |
| <local>        | Specifies the administrative distance of local BGP routes. These are routes redistributed from another protocol within your device. Specify the distance as a number between 1 and 255.<br>Default: <b>200</b>         |

**Mode [BGP]** Router Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage notes** You can use this command to set the administrative distance:

- for each BGP route type by specifying:

```
awplus(config-router)# distance <ebgp> <igbp> <local>
```

- for a specific route by specifying:

```
awplus(config-router)# distance <1-255> <ip-address/m>
[<listname>]
```

If the administrative distance is changed, it could create inconsistency in the routing table and obstruct routing.

**Example [BGP4+]** For BGP4+ IPv6, to set BGP 100's administrative distances for eBGP routes to 34, iBGP routes to 23, and local BGP routes to 15, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# distance bgp 34 23 15
```

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series



# exit-address-family

**Overview** Use this command to exit either the IPv4 or the IPv6 Address Family Configuration mode.

**Syntax** `exit-address-family`

**Mode [BGP]** IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Examples [BGP]** To enter and then exit IPv4 Address Family Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv4
awplus(config-router-af)# exit-address-family
awplus(config-router)#
```

**Example [BGP4+]** To enter and then exit IPv6 Address Family Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# exit-address-family
awplus(config-router)#
```

**Related commands** [address-family](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# ip community-list

**Overview** Use this command to add an entry to a standard or extended BGP community-list filter.

Use the **no** variant of this command to delete a standard or extended community list entry.

**Syntax** `ip community-list <listname> {deny|permit} .<community>`  
`no ip community-list <listname> {deny|permit} .<community>`

| Parameter    | Description                                                                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <listname>   | Specifies the community listname.                                                                                                                                                             |
| deny         | Specifies the community to reject.                                                                                                                                                            |
| permit       | Specifies the community to accept.                                                                                                                                                            |
| .<community> | {<AS:VAL> local-AS no-advertise no-export}                                                                                                                                                    |
| <AS:VAL>     | Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit format. |
| local-AS     | Specifies routes not to be advertised to external BGP peers.                                                                                                                                  |
| no-advertise | Specifies routes not to be advertised to other BGP peers.                                                                                                                                     |
| no-export    | Specifies routes not to be advertised outside of Autonomous System boundary.                                                                                                                  |

**Mode** Global Configuration

**Usage notes** A community-list can be used as a filter to BGP updates. Use this command to define the community access list globally, then use neighbor configuration commands to apply the list to a particular neighbor.

There are two kinds of community-lists: expanded and standard. A standard community-list defines the community attributes explicitly and not via a regular expression. An expanded community-list defines the communities attributes with regular expressions.

The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value that does not match the standard community value is automatically treated as expanded.

**Example** `awplus# configure terminal`  
`awplus(config)# ip community-list mylist permit 7675:80 7675:90`

**Related commands** [ip community-list standard](#)  
[ip community-list expanded](#)  
[show ip community-list](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# ip community-list expanded

**Overview** Use this command to add an entry to an expanded BGP community-list filter.

Use the **no** variant of this command to delete the community list entry.

**Syntax**

```
ip community-list <100-199> {deny|permit} .<line>
no ip community-list <100-199> {deny|permit} .<line>
ip community-list expanded <expanded-listname> {deny|permit}
.<line>
no ip community-list expanded <expanded-listname> {deny|permit}
.<line>
```

| Parameter           | Description                                              |
|---------------------|----------------------------------------------------------|
| <100-199>           | Expanded community list number.                          |
| expanded            | Specifies an expanded community list.                    |
| <expanded-listname> | Expanded community list entry.                           |
| deny                | Specifies community to reject.                           |
| permit              | Specifies community to accept.                           |
| .<line>             | Specifies community attributes with regular expressions. |

Regular expressions listed below can be used with the **ip community-list expanded** command:

| Symbo<br>l | Character     | Meaning                                                                                                                            |
|------------|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| ^          | Caret         | Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match. |
| \$         | Dollar sign   | Used to match the end of the input string.                                                                                         |
| .          | Period        | Used to match a single character (white spaces included).                                                                          |
| *          | Asterisk      | Used to match none or more sequences of a pattern.                                                                                 |
| +          | Plus sign     | Used to match one or more sequences of a pattern.                                                                                  |
| ?          | Question mark | Used to match none or one occurrence of a pattern.                                                                                 |
| _          | Underscore    | Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.                                    |
| [ ]        | Brackets      | Specifies a range of single-characters.                                                                                            |
| -          | Hyphen        | Separates the end points of a range.                                                                                               |

**Mode** Global Configuration

**Usage notes** A `community-list` can be used as a filter to BGP updates. Use this command to define the community access list globally, then use **neighbor** configuration commands to apply the list to a particular neighbor.

There are two kinds of community-lists: expanded and standard. A standard community-list defines the community attributes explicitly and not via a regular expression. An expanded community-list defines the communities attributes with regular expressions.

The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value that does not match the standard community value is automatically treated as expanded.

**Examples**

```
awplus# configure terminal
awplus(config)# ip community-list 125 permit 6789906
awplus(config)# ip community-list expanded CLIST permit .*
```

**Related commands**

- [ip community-list](#)
- [ip community-list standard](#)
- [show ip community-list](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# ip community-list standard

**Overview** Use this command to add an entry to a standard BGP community-list filter.  
Use the **no** variant of this command to delete the standard community-list entry.

**Syntax**

```
ip community-list <1-99> {deny|permit} [.<community>]
no ip community-list <1-99> {deny|permit} [.<community>]
ip community-list standard <standard-listname> {deny|permit}
[.<community>]
no ip community-list standard <standard-listname> {deny|permit}
[.<community>]
```

| Parameter           | Description                                                                                                                                                                                   |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-99>              | Standard community list number.                                                                                                                                                               |
| standard            | Specifies a standard community list.                                                                                                                                                          |
| <standard-listname> | Standard community list entry.                                                                                                                                                                |
| deny                | Specifies community to reject.                                                                                                                                                                |
| permit              | Specifies community to accept.                                                                                                                                                                |
| <community>         | {<AS:VAL>   local-AS   no-advertise   no-export}                                                                                                                                              |
| <AS:VAL>            | Specifies the valid value for the community number. This format represents the 32 bit communities value, where AS is the high order 16 bits and VAL is the low order 16 bits in digit format. |
| local-AS            | Specifies routes not to be advertised to external BGP peers.                                                                                                                                  |
| no-advertise        | Specifies routes not to be advertised to other BGP peers.                                                                                                                                     |
| no-export           | Specifies routes not to be advertised outside of the Autonomous System boundary.                                                                                                              |

**Mode** Global Configuration

**Usage notes** A community-list can be used as a filter to BGP updates. Use this command to define the community access list globally, then use neighbor configuration commands to apply the list to a particular neighbor.

There are two kinds of community-lists: expanded and standard. The standard community-list defines the community attributes as explicit values, without regular expressions. The expanded community-list defines the communities attributes with regular expressions.

The standard community-list is compiled into binary format and is directly compared with the BGP communities attribute in the BGP updates. The comparison is faster than the expanded community-list. Any community value

that does not match the standard community value is automatically treated as expanded.

**Examples**    `awplus# configure terminal`  
`awplus(config)# ip community-list standard CLIST permit 7675:80`  
`7675:90 no-export`  
`awplus(config)# ip community-list 34 permit 5675:50`  
`no-advertise`

**Related commands**    `ip community-list`  
`ip community-list expanded`  
`show ip community-list`

**Command changes**    Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# ip extcommunity-list expanded

**Overview** Use this command to create or delete an expanded extended community list.

Use the **no** variant of this command to delete the expanded extended community-list entry.

**Syntax**

```
ip extcommunity-list <100-199> {deny|permit}
{.<line>|. <AS:NN>|. <ip-address>}

no ip extcommunity-list <100-199> {deny|permit}
{.<line>|. <AS:NN>|. <ip-address>}

ip extcommunity-list expanded <expanded-listname> {deny|permit}
{.<line>|. <AS:NN>|. <ip-address>}

no ip extcommunity-list expanded <expanded-listname>
{deny|permit} {.<line>|. <AS:NN>|. <ip-address>}

no ip extcommunity-list <100-199>

no ip extcommunity-list expanded <expanded-listname>
```

| Parameter           | Description                                                                                                                                                                                       |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <100-199>           | Expanded extcommunity list number.                                                                                                                                                                |
| expanded            | Specifies an expanded extcommunity list.                                                                                                                                                          |
| <expanded-listname> | Expanded extcommunity list entry.                                                                                                                                                                 |
| deny                | Specifies the extcommunity to reject.                                                                                                                                                             |
| permit              | Specifies the extcommunity to accept.                                                                                                                                                             |
| .<line>             | Specifies extcommunity attributes with regular expression.                                                                                                                                        |
| <AS:NN>             | Specifies the valid value for an extcommunity number. This format represents the 32 bit extcommunities value, where AA is the high order 16 bits and NN is the low order 16 bits in digit format. |
| <ip-address>        | Specifies the IP address to deny or permit.                                                                                                                                                       |

Regular expressions listed below are used with the **ip extcommunity-list expanded** command:

| Symbol | Character   | Meaning                                                                                                                            |
|--------|-------------|------------------------------------------------------------------------------------------------------------------------------------|
| ^      | Caret       | Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match. |
| \$     | Dollar sign | Used to match the end of the input string.                                                                                         |



| Symbol | Character     | Meaning                                                                                         |
|--------|---------------|-------------------------------------------------------------------------------------------------|
| .      | Period        | Used to match a single character (white spaces included).                                       |
| *      | Asterisk      | Used to match none or more sequences of a pattern.                                              |
| +      | Plus sign     | Used to match one or more sequences of a pattern.                                               |
| ?      | Question mark | Used to match none or one occurrence of a pattern.                                              |
| —      | Underscore    | Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string. |
| [ ]    | Brackets      | Specifies a range of single-characters.                                                         |
| –      | Hyphen        | Separates the end points of a range.                                                            |

**Mode** Global Configuration

**Examples** `awplus# configure terminal`  
`awplus(config)# ip extcommunity-list 125 permit 4567335`  
`awplus(config)# ip extcommunity-list expanded CLIST permit .*`

**Related commands** [ip extcommunity-list standard](#)  
[show ip extcommunity-list](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# ip extcommunity-list standard

**Overview** Use this command to create and delete a standard extended community list.

Use the **no** variant of this command to delete a standard extended community-list entry.

**Syntax**

```
ip extcommunity-list <1-99> {deny|permit} {rt|soo}
<community-number>

ip extcommunity-list standard <standard-listname> {deny|permit}
{rt|soo} <community-number>

no ip extcommunity-list <1-99> [{deny|permit} {rt|soo}
<community-number>]

no ip extcommunity-list standard <standard-listname>
[{deny|permit} {rt|soo} <community-number>]
```

| Parameter           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-99>              | Standard extcommunity list number.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| standard            | Specifies a standard extended community list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <standard-listname> | Standard extended community list entry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| deny                | Specifies the extended community to reject.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| permit              | Specifies the extended community to accept.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| rt                  | Specifies the route target of the extended community.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| soo                 | Specifies the site of origin of the extended community.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <community-number>  | <p>Specifies the valid value for an extended community number.</p> <p>This can be one of two formats:</p> <ul style="list-style-type: none"><li>• &lt;ASN:NN&gt; where <i>ASN</i> is an AS (Autonomous System) number and <i>NN</i> is a value chosen by the ASN administrator</li><li>• &lt;A.B.C.D:NN&gt; where <i>A.B.C.D</i> is an IPv4 address, and <i>NN</i> is a value chosen by the ASN administrator.</li></ul> <p>Note that <i>ASN</i> and <i>NN</i> are both integers from 1 to 4294967295.</p> <p>AS numbers are assigned to the regional registries by IANA (<a href="http://www.iana.org">www.iana.org</a>) and must be obtained in your region.</p> |

**Mode** Global Configuration

**Examples**

```
awplus# configure terminal
awplus(config)# ip extcommunity-list 36 permit rt 5675:50
awplus(config)# ip extcommunity-list standard CLIST permit soo
7645:70
awplus# configure terminal
awplus(config)# ip extcommunity-list 36 deny rt 192.168.1.1:70
awplus(config)# ip extcommunity-list standard CLIST deny soo
10.10.1.1:50
```

**Related commands**

- [ip extcommunity-list expanded](#)
- [show ip extcommunity-list](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# ip prefix-list

**Overview** Use this command to create an entry for an IPv4 prefix list.

Use the **no** variant of this command to delete the IPv4 prefix-list entry.

**Syntax**

```
ip prefix-list <list-name> [seq <1-429496725>] {deny|permit}
{any|<ip-prefix>} [ge <0-32>] [le <0-32>]

ip prefix-list <list-name> description <text>

ip prefix-list sequence-number

no ip prefix-list <list-name> [seq <1-429496725>]

no ip prefix-list <list-name> [description <text>]

no ip prefix-list sequence-number
```

| Parameter         | Description                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------|
| <list-name>       | Specifies the name of a prefix list.                                                                 |
| seq <1-429496725> | Sequence number of the prefix list entry.                                                            |
| deny              | Specifies that the prefixes are excluded from the list.                                              |
| permit            | Specifies that the prefixes are included in the list.                                                |
| <ip-prefix>       | Specifies the IPv4 address and length of the network mask in dotted decimal in the format A.B.C.D/M. |
| any               | Any prefix match. Same as <b>0.0.0.0/0 le 32</b> .                                                   |
| ge<0-32>          | Specifies the minimum prefix length to be matched.                                                   |
| le<0-32>          | Specifies the maximum prefix length to be matched.                                                   |
| <text>            | Text description of the prefix list.                                                                 |
| sequence-number   | Specify sequence numbers included or excluded in prefix list.                                        |

**Mode** Global Configuration

**Usage notes** When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the **seq** parameter and place common permits or denials towards the top of the list. If you do not use the **seq** parameter, the sequence values are generated in a sequence of 5.

The parameters **ge** and **le** specify the range of the prefix lengths to be matched. When setting these parameters, set the **le** value to be less than 32, and the **ge** value to be less than or equal to the **le** value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.

**Example** In the following sample configuration, the last **ip prefix-list** command in the below list matches all, and the first **ip prefix-list** command denies the IP network 76.2.2.0:

```
awplus(config)# router bgp 100
awplus(config-router)# network 172.1.1.0
awplus(config-router)# network 172.1.2.0
awplus(config-router)# neighbor 10.6.5.3 remote-as 300
awplus(config-router)# neighbor 10.6.5.3 prefix-list mylist out
awplus(config-router)# exit
awplus(config)# ip prefix-list mylist seq 5 deny 76.2.2.0/24
awplus(config)# ip prefix-list mylist seq 100 permit any
```

To deny the IP addresses between 10.0.0.0/14 (10.0.0.0 255.252.0.0) and 10.0.0.0/22 (10.0.0.0 255.255.252.0) within the 10.0.0.0/8 (10.0.0.0 255.0.0.0) addressing range, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip prefix-list mylist seq 12345 deny 10.0.0.0/8
ge 14 le 22
```

**Related commands**

- [neighbor prefix-list](#)
- [clear ip prefix-list](#)
- [show ip prefix-list](#)

# ipv6 prefix-list

**Overview** Use this command to create an IPv6 prefix list or an entry in an existing prefix list.

Use the **no** variant of this command to delete a whole prefix list, a prefix list entry, or a description.

**Syntax**

```
ipv6 prefix-list <list-name> [seq <1-429496725>] {deny|permit}
{any|<ipv6-prefix>} [ge <0-128>] [le <0-128>]

ipv6 prefix-list <list-name> description <text>

no ipv6 prefix-list <list-name> [seq <1-429496725>]

no ipv6 prefix-list <list-name> [description <text>]
```

| Parameter         | Description                                                                          |
|-------------------|--------------------------------------------------------------------------------------|
| <list-name>       | Specifies the name of a prefix list.                                                 |
| seq <1-429496725> | Sequence number of the prefix list entry.                                            |
| deny              | Specifies that the prefixes are excluded from the list.                              |
| permit            | Specifies that the prefixes are included in the list.                                |
| <ipv6-prefix>     | Specifies the IPv6 prefix and prefix length in hexadecimal in the format X:X::X:X/M. |
| any               | Any prefix match. Same as ::0/0 le 128.                                              |
| ge <0-128>        | Specifies the minimum prefix length to be matched.                                   |
| le <0-128>        | Specifies the maximum prefix length to be matched.                                   |
| description       | Prefix list specific description.                                                    |
| <text>            | Up to 80 characters of text description of the prefix list.                          |

**Mode** Global Configuration

**Usage notes** When the device processes a prefix list, it starts to match prefixes from the top of the prefix list, and stops whenever a permit or deny occurs. To promote efficiency, use the **seq** parameter and place common permits or denials towards the top of the list. If you do not use the **seq** parameter, the sequence values are generated in a sequence of 5.

The parameters **ge** and **le** specify the range of the prefix lengths to be matched. The parameters **ge** and **le** are only used if an ip-prefix is stated. When setting these parameters, set the **le** value to be less than 128, and the **ge** value to be less than or equal to the **le** value and greater than the ip-prefix mask length.

Prefix lists implicitly exclude prefixes that are not explicitly permitted in the prefix list. This means if a prefix that is being checked against the prefix list reaches the end of the prefix list without matching a permit or deny, this prefix will be denied.

**Example** To check the first 32 bits of the prefix 2001:db8:: and that the subnet mask must be greater than or equal to 34 and less than or equal to 40, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 prefix-list mylist seq 12345 permit
2001:db8::/32 ge 34 le 40
```

**Related commands**

- match ipv6 address
- show ipv6 prefix-list
- show running-config ipv6 prefix-list

# match as-path

**Overview** Use this command to add an autonomous system (AS) path match clause to a route map entry. Specify the AS path attribute value or values to match by specifying the name of an AS path access list.

A BGP update message matches the route map if its attributes include AS path values that match the AS path access list.

Each entry of a route map can only match against one AS path access list in one AS path match clause. If the route map entry already has an AS path match clause, entering this command replaces that match clause with the new clause.

Note that AS path access lists and route map entries both specify an action of deny or permit. The action in the AS path access list determines whether the route map checks update messages for a given AS path value. The route map action and its **set** clauses determine what the route map does with update messages that contain that AS path value.

Use the **no** variant of this command to remove the AS path match clause from a route map entry.

**Syntax** `match as-path <as-path-listname>`  
`no match as-path [<as-path-listname>]`

| Parameter                             | Description                            |
|---------------------------------------|----------------------------------------|
| <code>&lt;as-path-listname&gt;</code> | Specifies an AS path access list name. |

**Mode** Route-map Configuration

**Usage notes** This command is valid for BGP update messages only.

**Example** To add entry 34 to the route map called `myroute`, which will discard update messages if they contain the AS path values that are included in `myaccesslist`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute deny 34
awplus(config-route-map)# match as-path myaccesslist
```

**Related commands** [route-map](#)  
[set as-path](#)  
[show route-map](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# match community

**Overview** Use this command to add a community match clause to a route map entry. Specify the community value or values to match by specifying a community list. To create the community list, enter Global Configuration mode and use the [ip community-list](#) command.

A BGP update message matches the route map if its attributes include community values that match the community list.

Each entry of a route map can only match against one community list in one community match clause. If the route map entry already has a community match clause, entering this command replaces that match clause with the new clause.

Note that community lists and route map entries both specify an action of deny or permit. The action in the community list determines whether the route map checks update messages for a given community value. The route map action and its **set** clauses determine what the route map does with update messages that contain that community value.

Use the **no** variant of this command to remove the community match clause from a route map.

**Syntax**

```
match community
{<community-listname>|<1-99>|<100-199>} [exact-match]

no match community
[<community-listname>|<1-99>|<100-199>|exact-match]
```

| Parameter            | Description                             |
|----------------------|-----------------------------------------|
| <community-listname> | The community list name or number.      |
| <1-99>               | Community list number (standard range). |
| <100-199>            | Community list number (expanded range). |
| exact-match          | Exact matching of communities.          |

**Mode** Route-map Configuration

**Usage notes** This command is valid for BGP update messages only.

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes.

**Example** To add entry 3 to the route map called `myroute`, which will process update messages if they contain the community values that are included in `mylist`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# match community mylist
```

**Related commands**

- `ip community-list`
- `route-map`
- `set comm-list delete`
- `set community`
- `show route-map`

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# max-paths

**Overview** Use this command to set the number of equal-cost multi-path (ECMP) routes for eBGP or iBGP. You can install multiple BGP paths to the same destination to balance the load on the forwarding path.

Use the **no** variant of this command to disable this feature.

**Syntax** max-paths {ebgp|ibgp} <2-64>  
no max-paths ebgp [<2-64>]  
no max-paths ibgp [<2-64>]

| Parameter | Description                     |
|-----------|---------------------------------|
| ebgp      | eBGP ECMP session.              |
| ibgp      | iBGP ECMP session.              |
| <2-64>    | Specifies the number of routes. |

**Mode** Global Configuration

**Usage notes** This command is available for the default BGP instance and for IPV4 and IPV6 unicast addresses.

**Example** awplus# configure terminal  
awplus(config)# router bgp 64501  
awplus(config-router)# max-paths ebgp 2

**Related commands** [show ip route summary](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor activate

**Overview** Use this command to enable the exchange of BGP IPv4 and BGP4+ IPv6 routes with a neighboring router, and also within either an IPv4 or an IPv6 specific address-family.

Use the **no** variant of this command to disable the exchange of information with a BGP or BGP4+ neighbor, in the Router Configuration or the Address Family Configuration mode.

**Syntax** neighbor <neighborid> activate  
no neighbor <neighborid> activate

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                              |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage [BGP]** Use this command to enable the exchange of information to a neighbor. To exchange IPv4 or IPv6 prefixes with a BGP or a BGP4+ peer, you must configure this command for the peer or the peer group. This command only enables the exchange of information. You can establish peering without this command, but no prefixes and other information is sent until you apply this command to the neighbor.

This command triggers the device to start a BGP or BGP4+ peering relationship with the specified BGP or BGP4+ neighbor and start exchanging routes with that neighbor.

**Examples [BGP]** To enable an exchange of routes with a neighboring router with the IPv4 address 10.10.10.1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 activate
```

To disable an exchange of routes with a neighboring router with the IPv4 address 10.10.10.1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 activate
```

To enable an exchange of routes in Address Family Configuration mode with a neighboring router with the IPv4 address 10.10.10.1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1 activate
```

To disable an exchange of routes in Address Family Configuration mode with a neighboring router with the IPv4 address 10.10.10.1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1 activate
```

To enable an exchange of routes with a neighboring router with the peer-group named group1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.63 remote-as 10
awplus(config-router)# neighbor 10.10.0.63 peer-group group1
awplus(config-router)# neighbor group1 activate
```

To disable an exchange of routes with a neighboring router with the peer-group named group1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 activate
```

**Examples**  
**[BGP4+]** To enable an exchange of routes in IPv6 Address Family Configuration mode with a neighboring router with the IPv6 address 2001:0db8:010d::1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1 activate
```

To disable an exchange of routes in IPv6 Address Family Configuration mode with a neighboring router with the IPv6 address 2001:0db8:010d::1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
activate
```

To enable an exchange of routes with a neighboring router with the peer-group named group1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 activate
```

To disable an exchange of routes with a neighboring router with the peer-group named group1, enter the commands as shown below:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 activate
```

**Related commands**   [neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command changes**   Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor advertisement-interval

**Overview** Use this command to set the minimum interval between sending iBGP or eBGP routing updates for a given route. This command reduces the flapping of individual routes.

Use the **no** variant of this command to set the interval time to the default values (30 seconds for eBGP peers and 5 seconds for iBGP peers) for a given route.

**Syntax** `neighbor <neighborid> advertisement-interval <time>`  
`no neighbor <neighborid> advertisement-interval [<time>]`

| Parameter                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;neighborid&gt;</code> | { <code>&lt;ip-address&gt;</code>   <code>&lt;ipv6-addr&gt;</code>   <code>&lt;peer-group&gt;</code> }                                                                                                                                                                                                                                                                                                                                            |
| <code>&lt;ip-address&gt;</code> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                                                                                                                                                  |
| <code>&lt;ipv6-addr&gt;</code>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                                                                                                                                                     |
| <code>&lt;peer-group&gt;</code> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. Note that if you apply an advertisement-interval value to a peer group it will apply to all members in the peer group. |
| <code>&lt;time&gt;</code>       | <code>&lt;0-600&gt;</code> Advertisement -interval value in seconds.                                                                                                                                                                                                                                                                                                                                                                              |

**Default** The default interval between sending routing updates for a given route to eBGP peers is 30 seconds, and the default interval for a given route to iBGP peers is 5 seconds.

**Mode** Router Configuration

**Usage notes** Use this command to set the minimum interval between sending iBGP or eBGP routing updates for a given route. To reduce the flapping of routes to the internet, set a minimum advertisement interval, so iBGP or eBGP routing updates are sent per interval seconds.

BGP dampening can also be used to control the effects of flapping routes. See the [bgp dampening](#) command in this chapter, and the [Routing\\_Protocol Guide](#) for more information.

The advertisement-interval time value is the minimum time between the advertisement of Update messages sent from a BGP speaker to report changes to

eBGP or iBGP peers. This is the minimum time between two Update messages sent to iBGP or eBGP peers.

See the [neighbor as-origination-interval](#) command to set the interval time between messages to iBGP peers, which have prefixes within the local AS. Use this command instead of the [neighbor as-origination-interval](#) command for eBGP peers with prefixes not in the same AS and updates not in a local AS.

#### Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.3
advertisement-interval 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.3
advertisement-interval
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.3 remote-as 10
awplus(config-router)# neighbor 10.10.0.3 peer-group group1
awplus(config-router)# neighbor group1 advertisement-interval
45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1
advertisement-interval
```



**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
advertisement-interval 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
advertisement-interval
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1
advertisement-interval 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1
advertisement-interval
```

**Related**  
**commands**

[neighbor as-origination-interval](#)  
[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)  
[show bgp ipv6 neighbors \(BGP4+ only\)](#)  
[show ip bgp neighbors \(BGP only\)](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor allowas-in

**Overview** Use this command to accept an AS\_PATH with the specified Autonomous System (AS) number from inbound updates for both BGP and BGP4+ routes.

This command allows BGP and BGP4+ to accept prefixes with the same ASN in the AS\_PATH attribute. This command allows BGP and BGP4+ to accept up to 10 instances, configured by the *<occurrences>* placeholder, of its own AN in the AS\_PATH for a prefix.

Use the **no** variant of this command to revert to default functionality (disabled by default).

**Syntax** `neighbor <neighborid> allowas-in <occurrences>`  
`no neighbor <neighborid> allowas-in`

| Parameter                  | Description                                                                                                                                                                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;neighborid&gt;</i>  | { <i>&lt;ip-address&gt;</i>   <i>&lt;ipv6-addr&gt;</i>   <i>&lt;peer-group&gt;</i> }                                                                                                                                                                                                                                       |
| <i>&lt;ip-address&gt;</i>  | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <i>&lt;ipv6-addr&gt;</i>   | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <i>&lt;peer-group&gt;</i>  | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <i>&lt;occurrences&gt;</i> | <i>&lt;1-10&gt;</i> Specifies the number of occurrences of the AS number.                                                                                                                                                                                                                                                  |

**Default** Disabled

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage** Use this command to configure PE (Provider Edge) routers to allow re-advertisement of all prefixes containing duplicate Autonomous System Numbers (ASNs). In a hub and spoke configuration, a PE router re-advertises all prefixes containing duplicate ASNs. Specify the remote-as or peer-group first using the related commands. The command allows a receiving peer to accept prefixes with its own AN in the AS\_PATH, up the maximum number of instances, as configured by the *<occurrences>* placeholder.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.1 allowas-in 3
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.0.1 allowas-in 3
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.1 allowas-in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.0.1 allowas-in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.1 remote-as 10
awplus(config-router)# neighbor 10.10.0.1 peer-group group1
awplus(config-router)# neighbor group1 allowas-in 3
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor group1 allowas-in 3
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
allowas-in 3

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
allowas-in

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 allowas-in 3

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor group1 allowas-in 3
```

**Related**  
**commands**

[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor as-origination-interval

**Overview** Use this command to adjust the sending of AS (Autonomous System) origination routing updates to a specified iBGP peer. This command adjusts the rate at which updates are sent to a specified iBGP peer (15 seconds by default). You must set a rate when you enable it.

The as-origination-interval is the minimum time set between the advertisement of Update messages sent from a BGP speaker to an iBGP peer to report changes within the local AS.

Use the **no** variant of this command to reset the timer to the default value of 15 seconds.

**Syntax [BGP]** `neighbor <neighbor_address> as-origination-interval <time>`  
`no neighbor <neighbor_address> as-origination-interval [<time>]`

**Syntax [BGP4+]** `neighbor <ipv6-addr> as-origination-interval <time>`  
`no neighbor <ipv6-addr> as-origination-interval [<time>]`

| Parameter          | Description                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------|
| <neighbor_address> | Specify a neighbor IPv4 address, in dotted decimal in the format A.B.C.D.                    |
| <ipv6-addr>        | Specify an address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X. |
| <time>             | <1-600> Time in seconds.                                                                     |

**Default** The default interval between sending routing updates to iBGP peers, which include a prefix that originates from the local AS, is 15 seconds by default.

**Mode** Router Configuration

**Usage** This command is used to change the minimum interval between sending AS-origination routing updates. The update interval for iBGP peers can be set from 1 to 600 seconds.

For interoperability with other vendors' devices, we recommend using the default value. The AS origination interval timer may not be available to adjust on other vendors' devices. Applying the default of 15 seconds across the AS maintains a common timer policy.

AlliedWare Plus devices use the default 15 second AS Origination Interval timer as per RFC 4271, a 30 second keepalive timer, a 90 second hold timer, a 120 second connect timer, a 5 second iBGP peer route advertisement interval, and a 30 second eBGP peer route advertisement interval.

Cisco devices use a 60 second keepalive timer, a 180 second hold timer, and no iBGP peer route interval timer (0). Juniper devices use a 10 second AS Origination Interval timer.

The as-origination-interval time value is the minimum amount of time between the advertisement of Update messages sent from a BGP speaker to report changes within the local AS. This is the minimum time between two Update messages to iBGP peers, which contain a prefix that originates from the same AS. See the [neighbor advertisement-interval](#) command to set time between messages to eBGP peers.

Use this command instead of the [neighbor advertisement-interval](#) command for iBGP peers with prefixes in the same AS for updates only within a local AS.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# neighbor 10.10.0.1
as-origination-interval 10
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no neighbor 10.10.0.1
as-origination-interval
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# neighbor 2001:0db8:010d::1
as-origination-interval 10
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-router)# no neighbor 2001:0db8:010d::1
as-origination-interval
```

**Validation Commands**

- [show bgp ipv6 neighbors](#) (BGP4+ only)
- [show ip bgp neighbors](#) (BGP only)

**Related commands**

- [neighbor advertisement-interval](#)
- [address-family](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor attribute-unchanged

**Overview** Use this command to advertise unchanged BGP or BGP4+ attributes to the specified BGP or BGP4+ neighbor.

Use the **no** variant of this command to disable this function.

**Syntax** `neighbor <neighborid> attribute-unchanged  
{as-path|next-hop|med}`  
`no neighbor <neighborid> attribute-unchanged  
{as-path|next-hop|med}`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | {<ip-address>   ipv6-addr>   <peer-group>}                                                                                                                                                                                                                                                                                 |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| as-path      | AS path attribute.                                                                                                                                                                                                                                                                                                         |
| next-hop     | Next hop attribute.                                                                                                                                                                                                                                                                                                        |
| med          | Multi Exit Discriminator.                                                                                                                                                                                                                                                                                                  |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage notes** Note that specifying this command with the optional **as-path** parameter has the same effect as invoking the [neighbor transparent-as](#) command.

Note this specifying this command with the optional **next-hop** parameter has the same effect as invoking the [neighbor transparent-next-hop](#) command.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.75 attribute-unchanged
as-path med

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.75
attribute-unchanged as-path med

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.0.75
attribute-unchanged as-path med

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.0.75
attribute-unchanged as-path med

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.75 remote-as 10
awplus(config-router)# neighbor 10.10.0.75 peer-group group1
awplus(config-router)# neighbor group1 attribute-unchanged
as-path med

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 attribute-unchanged
as-path med
```



**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
attribute-unchanged as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
attribute-unchanged as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 attribute-unchanged
as-path med
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1
attribute-unchanged as-path med
```

**Related**  
**commands**

[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)  
[neighbor transparent-as](#)  
[neighbor transparent-nexthop](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor capability graceful-restart

**Overview** Use this command to configure the device to advertise the Graceful Restart Capability to BGP and BGP4+ neighbors.

Use the **no** variant of this command to configure the device so it does not advertise the Graceful Restart Capability to its neighbor.

**Syntax** `neighbor <neighborid> capability graceful-restart`  
`no neighbor <neighborid> capability graceful-restart`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                              |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Default** Disabled

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage** Use the **neighbor capability graceful-restart** command to advertise to the BGP or BGP4+ neighbor routers the capability of graceful restart. First specify the BGP or BGP4+ neighbor's **remote-as** identification number as assigned by the neighbor router.

The graceful restart capability is advertised only when the graceful restart capability has been enabled using the [bgp graceful-restart](#) command.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.50 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.50 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.50 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.50 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.50 remote-as 10
awplus(config-router)# neighbor 10.10.10.50 peer-group group1
awplus(config-router)# neighbor group1 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 capability
graceful-restart
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
capability graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
capability graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 capability
graceful-restart
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 capability
graceful-restart
```

**Related**  
**commands**

[bgp graceful-restart](#)  
[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)  
[restart bgp graceful \(BGP only\)](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor capability orf prefix-list

**Overview** Use this command to advertise ORF (Outbound Route Filters) capability to neighbors. Use this command to dynamically filter updates. The BGP speaker can advertise a prefix list with prefixes it wishes the peer to prune or filter from outgoing updates.

Use the **no** variant of this command to disable this function.

**Syntax** `neighbor <neighborid> capability orf prefix-list  
{both|receive|send}`

`no neighbor <neighborid> capability orf prefix-list  
{both|receive|send}`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | {<ip-address>   <ipv6-addr>   <peer-group>}                                                                                                                                                                                                                                                                                |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| orf          | Advertises ORF capability to its neighbors.                                                                                                                                                                                                                                                                                |
| both         | Indicates that the local router can send ORF entries to its peer as well as receive ORF entries from its peer.                                                                                                                                                                                                             |
| receive      | Indicates that the local router is willing to receive ORF entries from its peer.                                                                                                                                                                                                                                           |
| send         | Indicates that the local router is willing to send ORF entries to its peer.                                                                                                                                                                                                                                                |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Default** Disabled

**Usage notes** Outbound Route Filters (ORFs) send and receive capabilities to lessen the number of updates exchanged between neighbors. By filtering updates, this option minimizes generating and processing of updates. The local router advertises the ORF capability in `send` mode and the remote router receives the ORF capability in

**receive** mode applying the filter as outbound policy. The two routers exchange updates to maintain the ORF for each router. Only an individual router or a peer-group can be configured to be in **receive** or **send** mode. A peer-group member cannot be configured in **receive** or **send** mode.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.5 capability orf
prefix-list both

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.5 capability orf
prefix-list both

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router)# neighbor 10.10.0.5 capability orf
prefix-list both

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router)# no neighbor 10.10.0.5 capability orf
prefix-list both

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.5 remote-as 10
awplus(config-router)# neighbor 10.10.0.5 peer-group group1
awplus(config-router)# neighbor group1 capability orf
prefix-list both

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 capability orf
prefix-list both
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router)# neighbor 2001:0db8:010d::1 capability
orf prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router)# no neighbor 2001:0db8:010d::1 capability
orf prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 capability orf
prefix-list both
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 capability orf
prefix-list both
```

**Related**  
**commands**

[neighbor capability orf prefix-list](#)  
[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor capability route-refresh

**Overview** Use this command to advertise route-refresh capability to the specified BGP and BGP4+ neighbors.

Use the **no** variant of this command to disable this function

**Syntax** `neighbor <neighborid> capability route-refresh`  
`no neighbor <neighborid> capability route-refresh`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                               |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode** Router Configuration

**Default** Enabled

**Usage** Use this command to advertise to peer about route refresh capability support. If route refresh capability is supported, then router can dynamically request that the peer readvertises its Adj-RIB-Out.



**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 capability
route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 capability
route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.1.1 remote-as 10
awplus(config-router)# neighbor 10.10.1.1 peer-group group1
awplus(config-router)# neighbor group1 capability route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 capability
route-refresh
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 capability
route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 capability
route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 capability route-refresh
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 capability
route-refresh
```

**Related commands**    [neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command changes**    Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor collide-established

**Overview** Use this command to specify including a BGP or BGP4+ neighbor, already in an 'established' state, for conflict resolution when a TCP connection collision is detected.

Use the **no** variant of this command to remove a BGP or BGP4+ neighbor, already in an 'established' state, for conflict resolution when a TCP connection collision is detected.

**Syntax** `neighbor <neighborid> collide-established`  
`no neighbor <neighborid> collide-established`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | {<ip-address> <ipv6-addr> <peer-group>}                                                                                                                                                                                                                                                                                    |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode** Router Configuration

**Usage notes** This command must be used only when specially required. It is not required in most network deployments.

The associated functionality of including an 'established' neighbor into TCP connection collision conflict resolution is automatically enabled when neighbor is configured for BGP graceful-restart.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1
collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 collide-established
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 collide-established
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 collide-established
```

**Related commands**

- [neighbor peer-group \(add a neighbor\)](#)
- [neighbor route-map](#)

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor default-originate

**Overview** Use this command to allow a BGP or BGP4+ local router to send the default route to a neighbor.

Use the **no** variant of this command to send no route as a default route.

**Syntax** `neighbor {<neighborid>} default-originate [route-map <routemap-name>]`  
`no neighbor {<neighborid>} default-originate [route-map <routemap-name>]`

| Parameter       | Description                                                                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid>    | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                                           |
|                 | <ip-address> Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
|                 | <ipv6-addr> Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                               |
|                 | <peer-group> Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| route-map       | If a route-map is specified, then the route table must contain at least one route that matches the permit criteria of the route map before the default route will be advertised to the specified neighbor.                                                                                                                              |
| <routemap-name> | Enter the route-map name.                                                                                                                                                                                                                                                                                                               |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Examples [BGP]** To allow a device to originate default route to neighbor 10.10.10.1, when the device's route table contains at least one route matching the route map 'myroute', use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 default-originate
route-map myroute
```

To stop a device from originating default route to neighbor 10.10.10.1, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 default-originate
route-map myroute
```

To allow a device to originate the IPv4 default route to neighbor 10.10.10.1, when the device's route table contains at least one route matching the route map 'myroute', use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1
default-originate route-map myroute
```

To stop a device from originating IPv4 default route to neighbor 10.10.10.1, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1
default-originate route-map myroute
```

To allow a device to originate default route to peer group 'group1', when the device's route table contains at least one route matching the route map 'myroute', use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 default-originate
route-map myroute
```

To stop a device originating default route to peer group 'group1', use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 default-originate
route-map myroute
```

**Examples** To allow a device to originate default route to neighbor 2001:0db8:010d::1, when  
**[BGP4+]** the device's route table contains at least one route matching the route map 'myroute', use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
default-originate route-map myroute
```

To stop a device originating default route to neighbor 2001:0db8:010d::1, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
default-originate route-map myroute
```

To allow a device to originate default route to peer group 'group1', when the device's route table contains at least one route matching the route map 'myroute', use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 default-originate
route-map myroute
```

To stop a device originating default route to peer group 'group1', use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 default-originate
route-map myroute
```

**Related commands** [neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# neighbor description

**Overview** Use this command to associate a description with a BGP or a BGP4+ neighbor. We recommend adding descriptions to defined neighbors, so any network administrators or network engineers can see a description of connected BGP or BGP4+ peers on the device.

Use the **no** variant of this command to remove the description from a BGP or a BGP4+ neighbor.

**Syntax** `neighbor <neighborid> description <description>`  
`no neighbor <neighborid> description [<description>]`

| Parameter                        | Description                                                                                                                                                                                                                                                                                                                |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;neighborid&gt;</code>  | { <code>&lt;ip-address&gt;</code>   <code>&lt;ipv6-addr&gt;</code>   <code>&lt;peer-group&gt;</code> }                                                                                                                                                                                                                     |
| <code>&lt;ip-address&gt;</code>  | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <code>&lt;ipv6-addr&gt;</code>   | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <code>&lt;peer-group&gt;</code>  | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <code>&lt;description&gt;</code> | Enter up to 80 characters of text describing the neighbor.                                                                                                                                                                                                                                                                 |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 description Backup
router for sales

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 description

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 description Backup
router for sales

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 description Backup
router for sales.
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 description
Backup router for sales

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
description

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 description Backup
router for sales

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 description Backup
router for sales
```

**Related commands**    [neighbor peer-group \(add a neighbor\)](#)  
                              [neighbor route-map](#)

**Command changes**    Added to AlliedWare Plus prior to 5.4.6-1  
                              Version 5.4.7-2.1: BGP support added for x510 and x550 series  
                              Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor disallow-infinite-holdtime

**Overview** Use this command to disallow the configuration of infinite holdtime for BGP and BGP4+.

Use the **no** variant of this command to allow the configuration of infinite holdtime for BGP or BGP4+.

**Syntax [BGP]** neighbor {<ip-address>} disallow-infinite-holdtime  
no neighbor {<ip-address>} disallow-infinite-holdtime

**Syntax [BGP4+]** neighbor {<ipv6-addr>} disallow-infinite-holdtime  
no neighbor {<ipv6-addr>} disallow-infinite-holdtime

| Parameter    | Description                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------|
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.              |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X. |

**Mode** Router Configuration

**Usage** This command enables the local BGP or BGP4+ speaker to reject holdtime “0” seconds from the peer during exchange of open messages or the user during configuration.

The **no** variant of this command allows the BGP speaker to accept “0” holdtime from the peer or during configuration.

**Examples [BGP]** To enable the **disallow-infinite-holdtime** feature on the BGP speaker with the IP address of 10.10.10.1, enter the command:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1
disallow-infinite-holdtime
```

To disable the **disallow-infinite-holdtime** feature on the BGP speaker with the IP address of 10.10.10.10, enter the command:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1
disallow-infinite-holdtime
```

**Examples** To enable the **disallow-infinite-holdtime** feature on the BGP4+ speaker with the  
**[BGP4+]** IPv6 address of 2001:0db8:010d::1, enter the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor
disallow-infinite-holdtime2001:0db8:010d::1
```

To disable the **disallow-infinite-holdtime** feature on the BGP4+ speaker with the IPv6 address of 2001:0db8:010d::1, enter the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor
disallow-infinite-holdtime2001:0db8:010d::1
```

**Related commands** [neighbor timers](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor dont-capability-negotiate

**Overview** Use this command to disable capability negotiation for BGP and BGP4+.

The capability negotiation is performed by default. This command is used to allow compatibility with older BGP versions that have no capability parameters used in open messages between peers.

Use the **no** variant of this command to enable capability negotiation.

**Syntax** `neighbor <neighborid> dont-capability-negotiate`  
`no neighbor <neighborid> dont-capability-negotiate`

| Parameter    | Description                                                                                                                                                                                                                                                                                                        |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                      |
| <ip-address> | Specify the IPv4 address of the BGP neighbor in dotted decimal, in the format A.B.C.D.                                                                                                                                                                                                                             |
| <ipv6-addr>  | Specify the IPv6 address of the BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                     |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> and <a href="#">neighbor route-map</a> commands. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode** Router Configuration

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.34
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.34
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.34 remote-as 100
awplus(config-router)# neighbor 10.10.10.34 peer-group group1
awplus(config-router)# neighbor group1
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1
dont-capability-negotiate
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1
dont-capability-negotiate
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1
dont-capability-negotiate
```

**Related commands**    `neighbor peer-group` (add a neighbor)  
                          `neighbor route-map`

**Command changes**    Added to AlliedWare Plus prior to 5.4.6-1  
                          Version 5.4.7-2.1: BGP support added for x510 and x550 series  
                          Version 5.4.7-2.4: BGP support added for IE300 series



# neighbor ebgp-multihop

**Overview** Use this command to accept and attempt BGP or BGP4+ connections to external peers on indirectly connected networks.

Effectively, this command sets the TTL value in the BGP or BGP4+ packets that the router sends to the neighbor, so that the packets may traverse the network route to the neighbor.

The device will not establish a connection to a multihop neighbor, if the only route to the multihop peer is a default route.

Use the **no** variant of this command to return to the default.

**Syntax** `neighbor <neighborid> ebgp-multihop [<count>]`  
`no neighbor <neighborid> ebgp-multihop [<count>]`

| Parameter                       | Description                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;neighborid&gt;</code> | <code>{ &lt;ip-address   ipv6-addr   &lt;peer-group&gt; }</code>                                                                                                                                                                                                                                                           |
| <code>&lt;ip-addr&gt;</code>    | Specify the address of an IPv4 BGP neighbor, entered in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                   |
| <code>&lt;ipv6-addr&gt;</code>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <code>&lt;peer-group&gt;</code> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <code>&lt;count&gt;</code>      | <code>&lt;1-255&gt;</code> The Maximum hop count, that is set in the TTL field of the BGP packets. If this optional parameter is not specified with the command, then the Maximum hop count is set to 255.                                                                                                                 |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.34 remote-as 10
awplus(config-router)# neighbor 10.10.10.34 ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.34 ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.34 remote-as 10
awplus(config-router)# neighbor 10.10.10.34 peer-group group1
awplus(config-router)# neighbor group1 ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 ebgp-multihop 5
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# neighbor 2001:0db8:010d::1
ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 ebgp-multihop 5
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 ebgp-multihop 5
```

**Related commands**    [neighbor ebgp-multihop](#)  
                          [neighbor peer-group \(add a neighbor\)](#)  
                          [neighbor route-map](#)

**Command changes**    Added to AlliedWare Plus prior to 5.4.6-1  
                              Version 5.4.7-2.1: BGP support added for x510 and x550 series  
                              Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor enforce-multihop

**Overview** Use this command to enforce the requirement that BGP and BGP4+ neighbors form multihop connections.

Use the **no** variant of this command to turn off this feature.

**Syntax** `neighbor <neighborid> enforce-multihop`  
`no neighbor <neighborid> enforce-multihop`

| Parameter    | Description                                                                                                                                                                                                                                                                                                      |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | {<ip-address> <ipv6-addr> <peer-group>}                                                                                                                                                                                                                                                                          |
| <ip-address> | The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                         |
| <ipv6-addr>  | The address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                            |
| <peer-group> | Name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.34 remote-as 10
awplus(config-router)# neighbor 10.10.0.34 enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.34 enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.34 remote-as 10
awplus(config-router)# neighbor 10.10.10.34 peer-group group1
awplus(config-router)# neighbor group1 enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 enforce-multihop
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# neighbor 2001:0db8:010d::1
enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 enforce-multihop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 enforce-multihop
```

**Related commands**   [neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command changes**   Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor filter-list

**Overview** This command creates a BGP or BGP4+ filter using an AS (Autonomous System) path list. This command specifies an AS path list, which it then applies to filter updates to and from a BGP or a BGP4+ neighbor

The **no** variant of this command removes the previously specified BGP or BGP4+ filter using access control lists.

**Syntax** `neighbor <neighborid> filter-list <listname> {in|out}`  
`no neighbor <neighborid> filter-list <listname> {in|out}`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | Specify the identification method for the BGP or BGP4+ peer. Use one of the following formats:                                                                                                                                                                                                                                          |
|              | <ip-address> Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
|              | <ipv6-addr> Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                               |
|              | <peer-group> Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <listname>   | Specify the name of an AS (Autonomous System) path list.                                                                                                                                                                                                                                                                                |
| in           | Indicates that incoming advertised routes will be filtered.                                                                                                                                                                                                                                                                             |
| out          | Indicates that outgoing advertised routes will be filtered.                                                                                                                                                                                                                                                                             |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage** This command specifies a filter for updates based on a BGP AS (Autonomous System) path list.

### Examples [BGP]

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.34 filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.34 filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.0.34 filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.0.34 filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.34 remote-as 10
awplus(config-router)# neighbor 10.10.10.34 peer-group group1
awplus(config-router)# neighbor group1 filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 filter-list list1 out
```



**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 filter-list list1 out
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 filter-list list1
out
```

**Related**  
**commands**

[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor interface

**Overview** Use this command to configure the interface name of a BGP4+ speaking neighbor. Use the **no** variant of this command to disable this function.

**Syntax [BGP4+]** neighbor {<ipv6-addr>|<ipaddress>} interface <interface>  
no neighbor {<ipv6-addr>|<ipaddress>} interface <interface>

| Parameter   | Description                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------|
| <ipaddress> | Specifies the IPv4 address of the BGP neighbor - entered in dotted decimal notation in the format A.B.C.D. |
| <ipv6-addr> | Specifies the IPv6 address of the BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.           |
| <interface> | Specifies the name of the interface to reach the BGP neighbor over.                                        |

**Mode [BGP4+]** Router Configuration

**Usage [BGP4+]** This command is for use with BGP4+ peering. Use this command for BGP peering with IPv6 link local addresses.

**Examples [BGP4+]** To specify a neighbor of 10.10.0.72 over the interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 interface eth1
```

To remove the neighbor of 10.10.0.72 over the interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 interface eth1
```

To specify a neighbor of 2001:0db8:010d::1 over the interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 interface eth1
```

To remove the neighbor of 2001:0db8:010d::1 over the interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 interface eth1
```

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor local-as

**Overview** Use this command to configure a local AS number for the specified BGP or BGP4+ neighbor. This overrides the local AS number specified by the [router bgp](#) command.

Use the **no** variant of this command to remove the local AS number for the specified BGP or BGP4+ neighbor.

**Syntax** `neighbor <neighborid> local-as <as-number>`  
`no neighbor <neighborid> local-as <as-number>`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                     |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                                   |
|              | <ip-address> The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
|              | <ipv6-addr> The address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                               |
|              | <peer-group> Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> and <a href="#">neighbor route-map</a> commands. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <as-number>  | <1-4294967295> Neighbor's Autonomous System (AS) number.                                                                                                                                                                                                                                                                        |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Usage [BGP4+]** When BGP4+ is configured, this command prepends the ASN as defined by the [router bgp](#) command, and adds the ASN as defined by the [neighbor local-as](#) command in front of the actual ASN as defined by the [router bgp](#) command. This makes the peer believe it is peering with the ASN as defined by the [neighbor local-as](#) command.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.34 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.34 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.34 remote-as 10
awplus(config-router)# neighbor 10.10.10.34 peer-group group1
awplus(config-router)# neighbor group1 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 local-as 1
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 local-as 1
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 local-as 1
```

**Related commands**

- [neighbor peer-group \(add a neighbor\)](#)
- [neighbor route-map](#)
- [router bgp](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor maximum-prefix

**Overview** Use this command to control the number of prefixes that can be received from a BGP or a BGP4+ neighbor.

Use the **no** variant of this command to disable this function. Do not specify threshold to apply the default threshold of 75% for the maximum number of prefixes before this is applied.

**Syntax** `neighbor <neighborid> maximum-prefix <maximum>`  
`no neighbor <neighborid> maximum-prefix [<maximum>]`

| Parameter                       | Description                                                                                                                                                                                                                                                                                                      |
|---------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;neighborid&gt;</code> | <code>{&lt;ip-address&gt;   &lt;ipv6-addr&gt;   &lt;peer-group&gt;}</code>                                                                                                                                                                                                                                       |
| <code>&lt;ip-address&gt;</code> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                 |
| <code>&lt;ipv6-addr&gt;</code>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                    |
| <code>&lt;peer-group&gt;</code> | Name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <code>&lt;maximum&gt;</code>    | <code>&lt;maxprefix&gt; [&lt;threshold&gt;] [warning-only]</code>                                                                                                                                                                                                                                                |
| <code>&lt;maxprefix&gt;</code>  | <code>&lt;1-4294967295&gt;</code><br>Specifies the maximum number of prefixes permitted.                                                                                                                                                                                                                         |
| <code>&lt;threshold&gt;</code>  | <code>&lt;1-100&gt;</code> Specifies the threshold value, 1 to 100 percent. 75% by default.                                                                                                                                                                                                                      |
| <code>warning-only</code>       | Only gives a warning message when the limit is exceeded.                                                                                                                                                                                                                                                         |

**Default** The default threshold value is 75%. If the threshold value is not specified this default is applied.

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage** The **neighbor maximum-prefix** command allows the configuration of a specified number of prefixes that a BGP or a BGP4+ router is allowed to receive from a neighbor. When the `warning-only` option is not used, if any extra prefixes are received, the router ends the peering. A terminated peer, stays down until the **clear ip bgp** command is used.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 maximum-prefix 1244
warning-only

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 maximum-prefix
1244 warning-only

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.72 remote-as 10
awplus(config-router)# neighbor 10.10.10.72 peer-group group1
awplus(config-router)# neighbor group1 maximum-prefix 1244
warning-only

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 maximum-prefix 1244
warning-only
```



**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
maximum-prefix 1244 warning-only
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
maximum-prefix 1244 warning-only
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 maximum-prefix 1244
warning-only
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 maximum-prefix
1244 warning-only
```

**Related  
commands**

[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor next-hop-self

**Overview** Use this command to configure the BGP or BGP4+ router as the next hop for a BGP or BGP4+ speaking neighbor or peer group.

Use the **no** variant of this command to disable this feature.

**Syntax** `neighbor <neighborid> next-hop-self`  
`no neighbor <neighborid> next-hop-self`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                              |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage notes** This command allows a BGP or BGP4+ router to change the next hop information that is sent to the iBGP peer. The next hop information is set to the IP address of the interface used to communicate with the neighbor.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router)# neighbor 10.10.0.72 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router)# no neighbor 10.10.0.72 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.72 remote-as 10
awplus(config-router)# neighbor 10.10.10.72 peer-group group1
awplus(config-router)# neighbor group1 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 next-hop-self
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 next-hop-self
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 next-hop-self
```

**Related**  
**commands**

[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor override-capability

**Overview** Use this command to override a capability negotiation result for BGP and BGP4+. Use the **no** variant of with this command to disable this function.

**Syntax** neighbor <neighborid> override-capability  
no neighbor <neighborid> override-capability

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | {<ip-address>   <ipv6-addr>   <peer-group>}                                                                                                                                                                                                                                                                                |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode** Router Configuration

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 override-capability
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72
override-capability
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.72 remote-as 10
awplus(config-router)# neighbor 10.10.10.72 peer-group group1
awplus(config-router)# neighbor group1 override-capability
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 override-capability
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor 2001:0db8:010d::1
override-capability
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor 2001:0db8:010d::1
override-capability
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 override-capability
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor group1 override-capability
```

**Related**  
**commands**

[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor passive

**Overview** Use this command to configure the local BGP or BGP4+ router to be passive with regard to the specified BGP or BGP4+ neighbor. This has the effect that the BGP or BGP4+ router will not attempt to initiate connections to this BGP or BGP4+ neighbor, but will accept incoming connection attempts from the BGP or BGP4+ neighbor.

Use the **no** variant of this command to disable this function.

**Syntax** `neighbor <neighborid> passive`  
`no neighbor <neighborid> passive`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                              |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.72 remote-as 10
awplus(config-router)# neighbor 10.10.10.72 peer-group group1
awplus(config-router)# neighbor group1 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 passive
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 passive
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 passive
```

**Related commands** [neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series



## Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor password

**Overview** Use this command to enable MD5 authentication on a TCP connection between BGP and BGP4+ neighbors. No authentication is applied by default. To setup authentication for the session, you must first apply authentication on each connected peer for the session.

Use the **no** variant of this command to disable this function.

**Syntax [BGP]** `neighbor {<ip-address>|<peer-group-name>} password <password>`  
`no neighbor {<ip-address>|<peer-group-name>} password`  
`[<password>]`

**Syntax [BGP4+]** `neighbor {<ipv6-addr>|<peer-group-name>} password <password>`  
`no neighbor {<ipv6-addr>|<peer-group-name>} password`  
`[<password>]`

| Parameter         | Description                                                                                                                             |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| <ip-address>      | Specifies the IP address of the BGP neighbor, in A.B.C.D format.                                                                        |
| <ipv6-addr>       | Specifies the IPv6 address of the BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                        |
| <peer-group-name> | Name of an existing peer-group. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <password>        | An alphanumeric string of characters to be used as password.                                                                            |

**Default** No authentication is applied by default.

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Usage notes** When using the <peer-group-name> parameter with this command (to apply this command to all peers in the group), see the related commands [neighbor peer-group \(add a neighbor\)](#) and [neighbor route-map](#) for information about how to create peer groups first.

**Examples [BGP]** This example specifies the encryption type and the password 'manager' for the neighbor 10.10.10.1:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 password manager
```

This example removes the password set for the neighbor 10.10.10.1:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 password
```

This example specifies the encryption type and the password 'manager' for the neighbor peer group named 'group1':

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 password manager
```

This example removes the password set for the neighbor peer group named group1:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 password
```

#### **Examples [BGP4+]**

This example specifies the encryption type and the password 'manager' for the neighbor 2001:0db8:010d::1:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor password manager
2001:0db8:010d::1
```

This example removes the password set for the neighbor 2001:0db8:010d::1:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor password 2001:0db8:010d::1
```

This example specifies the encryption type and the password 'manager' for the neighbor peer group named group1:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor remote-as 102001:0db8:010d::1
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor peer-group group1
2001:0db8:010d::1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 password manager
```

This example removes the password set for the neighbor peer group named 'group1':

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 password
```

**Related commands**   [neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command changes**   Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor peer-group (add a neighbor)

**Overview** Use this command to add a BGP or a BGP4+ neighbor to an existing peer-group.  
Use the **no** variant of this command to disable this function.

**Syntax [BGP]** `neighbor <ip-address> peer-group <peer-group>`  
`no neighbor <ip-address> peer-group <peer-group>`

**Syntax [BGP4+]** `neighbor <ipv6-addr> peer-group <peer-group>`  
`no neighbor <ipv6-addr> peer-group <peer-group>`

| Parameter    | Description                                                                                                                               |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-address> | Specify the IPv4 address of the BGP neighbor, entered in the format A.B.C.D.                                                              |
| <ipv6-addr>  | Specify the IPv6 address of the BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                            |
| <peer-group> | Enter the name of the peer-group. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage** Use this command to add neighbors with the same update policies to a peer group. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with many of the neighbor commands. Any changes made to the peer group affect all members.

To create a peer-group use the [neighbor port](#) command and then use this command to add neighbors to the group.

**Examples [BGP]** This example shows a new peer-group `group1` and the addition of a neighbor `10.10.0.63` to the group.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.63 peer-group group1
```

This example shows a new peer-group `group1` and the removal of a neighbor `10.10.0.63` to the group.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# no neighbor 10.10.0.63 peer-group group1
```

**Examples [BGP4+]** This example shows a new peer-group `group1` and the addition of a neighbor `2001:0db8:010d::1` to the group.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor peer-group
group1 2001:0db8:010d::1
```

This example shows a new peer-group `group1` and the removal of a neighbor `2001:0db8:010d::1` to the group.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor peer-group
group1 2001:0db8:010d::1
```

**Related commands** [neighbor peer-group \(create a peer-group\)](#)  
[neighbor port](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor peer-group (create a peer-group)

**Overview** Use this command to create a peer-group for BGP and BGP4+. Use the **no** variant of this command to disable this function.

**Syntax** `neighbor <peer-group> peer-group`  
`no neighbor <peer-group> peer-group`

| Parameter                       | Description                       |
|---------------------------------|-----------------------------------|
| <code>&lt;peer-group&gt;</code> | Enter the name of the peer-group. |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Usage notes** Neighbors with the same update policies are grouped into peer groups. This facilitates the updates of various policies, such as, distribute and filter lists. The peer-group is then configured easily with many of the neighbor commands. Any changes made to the peer group affect all members. Use this command to create a peer-group, then use the [neighbor peer-group \(add a neighbor\)](#) command to add neighbors to the group.

**Examples** `awplus# configure terminal`  
`awplus(config)# router bgp 10`  
`awplus(config-router)# neighbor group1 peer-group`  
`awplus# configure terminal`  
`awplus(config)# router bgp 10`  
`awplus(config-router)# no neighbor group1 peer-group`

**Related commands** [neighbor peer-group \(add a neighbor\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor port

**Overview** Use this command to specify the TCP port to which packets are sent to on a BGP or a BGP4+ neighbor. TCP port 179 is the default port used to connect BGP and BGP4+ peers. You can specify a different destination port for the TCP session with this command.

Use the **no** variant of this command to reset the port number back to the default value (TCP port 179).

**Syntax [BGP]** `neighbor <neighborid> port <portnum>`  
`no neighbor <neighborid> port [<portnum>]`

| Parameter                       | Description                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;neighborid&gt;</code> | { <code>&lt;ip-address&gt;</code>   <code>ipv6-addr</code>   <code>&lt;peer-group&gt;</code> }                                                                                                                                                                                                                             |
| <code>&lt;ip-address&gt;</code> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <code>&lt;ipv6-addr&gt;</code>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <code>&lt;peer-group&gt;</code> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <code>&lt;portnum&gt;</code>    | <code>&lt;0-65535&gt;</code> Specifies the TCP port number.                                                                                                                                                                                                                                                                |

**Default** TCP port 179 is the default port used to connect BGP and BGP4+ peers.

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration



**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor 10.10.10.10 port 643
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor 10.10.10.10 port 643
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 port 643
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor group1 port 643
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor port 643 2001:0db8:010d::1
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor port 643 2001:0db8:010d::1
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(awplus-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 port 643
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor group1 port 643
```

**Related commands** [neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series

## Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor prefix-list

**Overview** Use this command to distribute BGP and BGP4+ neighbor information as specified in a prefix list.

Use the **no** variant of this command to remove an entry.

**Syntax** `neighbor <neighborid> prefix-list <listname> {in|out}`  
`no neighbor <neighborid> prefix-list <listname> {in|out}`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | <ip-address> <ipv6-addr> <peer-group>                                                                                                                                                                                                                                                                                                   |
|              | <ip-address> Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
|              | <ipv6-addr> Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                               |
|              | <peer-group> Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <listname>   | The name of an IP prefix list.                                                                                                                                                                                                                                                                                                          |
| in           | Specifies that the IP prefix list applies to incoming advertisements.                                                                                                                                                                                                                                                                   |
| out          | Specifies that the IP prefix list applies to outgoing advertisements.                                                                                                                                                                                                                                                                   |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage notes** Use this command to specify a prefix list for filtering BGP or BGP4+ advertisements. Filtering by prefix list matches the prefixes of routes with those listed in the prefix list. If there is a match, the route is used. An empty prefix list permits all prefixes. If a given prefix does not match any entries of a prefix list, the route is denied access.

The router begins the search at the top of the prefix list, with the sequence number 1. Once a match or deny occurs, the router does not need to go through the rest of the prefix list. For efficiency the most common matches or denies are listed at the top.

The **neighbor distribute-list** command is an alternative to the **neighbor prefix-list** command and only one of them can be used for filtering to the same neighbor in any direction.

### Examples [BGP]

```
awplus# configure terminal
awplus(config)# ip prefix-list list1 deny 30.0.0.0/24
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 prefix-list list1 in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 prefix-list list1
in
awplus# configure terminal
awplus(config)# ip prefix-list list1 deny 30.0.0.0/24
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1 prefix-list list1
in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1 prefix-list
list1 in
awplus# configure terminal
awplus(config)# ip prefix-list list1 deny 30.0.0.0/24
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 prefix-list list1 in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 prefix-list list1 in
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# ipv6 prefix-list list1 deny
2001:0db8:010d::1/128

awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:: prefix-list
list1 in

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:: prefix-list
list1 in

awplus# configure terminal
awplus(config)# ip prefix-list list1 deny 2001:0db8:010d::1/128
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 prefix-list list1 in
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 prefix-list list1
in
```

**Related**  
**commands**

[ip prefix-list](#)  
[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor remote-as

**Overview** Use this command to configure an internal BGP or BGP4+ (iBGP or eBGP) peering relationship with another router.

Use the **no** variant of this command to remove a previously configured BGP or BGP4+ peering relationship.

**Syntax** `neighbor <neighborid> remote-as <as-number>`  
`no neighbor <neighborid> remote-as <as-number>`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   ipv6-addr   <peer-group> }                                                                                                                                                                                                                                                                                             |
|              | <ip-address> Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
|              | <ipv6-addr> Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                               |
|              | <peer-group> Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <as-number>  | <1-4294967295> Neighbor's Autonomous System (AS) number.                                                                                                                                                                                                                                                                                |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Usage notes** This command is used to configure iBGP and eBGP peering relationships with other BGP or BGP4+ neighbors. A peer-group support of this command is configured only after creating a specific peer-group. Use the **no** variant of this command to remove a previously configured BGP peering relationship.

**Examples [BGP]** To configure a BGP peering relationship from the neighbor with the IPv4 address 10.10.0.73 with another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.73 remote-as 10
```

To remove a configured BGP peering relationship from the neighbor with the IPv4 address 10.10.0.73 from another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.73 remote-as 10
```

To configure a BGP peering relationship from the neighbor with the peer group named group1 with another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 remote-as 10
```

To remove a configured BGP peering relationship from the neighbor with the peer group named group1 with another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 remote-as 10
```

#### **Examples [BGP4+]**

To configure a BGP4+ peering relationship with another router:

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 345
```

To remove a configured BGP4+ peering relationship from another router:

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# no neighbor 2001:0db8:010d::1 remote-as 345
```

To configure a BGP4+ peering relationship from the neighbor with the peer group named group1 with another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 remote-as 10
```

To remove a configured BGP4+ peering relationship from the neighbor with the peer group named group1 with another router:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 remote-as 10
```

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series



# neighbor remove-private-AS (BGP only)

**Overview** Use this command to remove the private Autonomous System (AS) number from external outbound updates. Use the **no** variant of this command to revert to the default (disabled).

**Syntax** `neighbor <neighborid> remove-private-AS`  
`no neighbor <neighborid> remove-private-AS`

| Parameter    | Description                                                                                                                                                                                                                                                                                                   |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <tag> }                                                                                                                                                                                                                                                                                      |
| <ip-address> | The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                      |
| <tag>        | Name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor remote-as</a> command. When this parameter is used with a command, the command applies on all peers in the specified group. |

**Default** This command is disabled by default.

**Mode** Router Configuration or IPv4 Address Family Configuration

**Usage notes** The private AS numbers range from <64512-65535>. Private AS numbers are not advertised to the Internet. This command is used with external BGP peers only. The router removes the AS numbers only if the update includes private AS numbers. If the update includes both private and public AS numbers, the system treats it as an error.

This command removes private AS numbers for BGP in Router Configuration mode. This command is not supported for BGP4+ in IPv6 Address Family Configuration mode. This command removes a private AS number and makes an update packet with a public AS number as the AS path attribute. So only public AS numbers are entered in Internet BGP routing tables, and private AS numbers are not entered in Internet BGP tables.

For the filtering to apply, both peering devices must be set to use either 2-byte or extended 4- byte ASN (with the same ASN type set on both peers). For example, if a device (which defaults to use a 4-byte ASN), is peered with a device that defaults to a 2-byte ASN, then the device using a 2-byte ASN device also needs to be configured with the command **bgp extended-asn-cap** for the filtering to apply.

**Examples**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.63 remove-private-AS
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.63 remove-private-AS
```

**Related commands** [show ip bgp \(BGP only\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor restart-time

**Overview** Use this command to set a different restart-time other than the global restart-time configured using the **bgp graceful-restart** command for BGP and BGP4+.

Use the **no** variant of this command to restore the device to its default state (see the default value of the **bgp graceful-restart** command).

**Syntax** `neighbor <neighborid> restart-time <delay-value>`  
`no neighbor <neighborid> restart-time <delay-value>`

| Parameter                        | Description                                                                                                                                                                                                                                                                                                                |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;neighborid&gt;</code>  | <code>{&lt;ip-address&gt;   &lt;ipv6-addr&gt;   &lt;peer-group&gt;}</code>                                                                                                                                                                                                                                                 |
| <code>&lt;ip-address&gt;</code>  | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <code>&lt;ipv6-addr&gt;</code>   | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <code>&lt;peer-group&gt;</code>  | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <code>&lt;delay-value&gt;</code> | <code>&lt;1-3600&gt;</code> Delay value in seconds.                                                                                                                                                                                                                                                                        |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Usage** This command takes precedence over the restart-time value specified using the **bgp graceful-restart** command.

The restart-time value is the maximum time that a graceful-restart neighbor waits to come back up after a restart. The default is 120 seconds.

Make sure that the restart time specified using this command does not exceed the stalepath-time specified in the Router Configuration mode.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 restart-time 45
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1 peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 restart-time 45
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 restart-time 45
```

**Related commands**

- [bgp graceful-restart](#)
- [neighbor peer-group \(add a neighbor\)](#)
- [neighbor route-map](#)

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor route-map

**Overview** Use this command to apply a route map to incoming or outgoing routes for BGP or BGP4+.

Use the **no** variant of this command to remove a route map from a BGP or BGP4+ route.

**Syntax** `neighbor <neighborid> route-map <mapname> {in|out}`  
`no neighbor <neighborid> route-map <mapname> {in|out}`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | {<ip-address>   ipv6-addr>   <peer-group>}                                                                                                                                                                                                                                                                                 |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <mapname>    | Specifies name of the route-map.                                                                                                                                                                                                                                                                                           |
| in           | Specifies that the access list applies to incoming advertisements.                                                                                                                                                                                                                                                         |
| out          | Specifies that the access list applies to outgoing advertisements.                                                                                                                                                                                                                                                         |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage notes** Use the **neighbor route-map** command to filter updates and modify attributes. A route map is applied to inbound or outbound updates. Only the routes that pass the route map are sent or accepted in updates.

**Examples [BGP]** The following example shows the configuration of the route-map name **rmap2** and then the use of this map name in the **neighbor route-map** command for the neighbor with the IPv4 address 10.10.10.1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 6
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 route-map rmap2 in
```

The following example shows the removal of the route-map name **rmap2** in the **neighbor route-map** command for the neighbor with the IPv4 address 10.10.10.1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 route-map rmap2 in
```

The following example shows the configuration of the route-map name **rmap2** and then the use of this map name in the **neighbor route-map** command for the neighbor with the IPv4 address 10.10.10.1 in the IPv4 Address Family Configuration mode.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 6
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1 route-map rmap2 in
```

The following example shows the removal of the route-map name **rmap2** in the **neighbor route-map** command for the neighbor with the IPv4 address 10.10.10.1 in the IPv4 Address Family Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1 route-map rmap2 in
```

The following example shows the configuration of the route-map name **rmap2** and then the use of this map name in the **neighbor route-map** command for the neighbor with the peer group named group1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 6
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 route-map rmap2 in
```

The following example shows the removal the route-map name **rmap2** in the **neighbor route-map** command for the neighbor with the peer group named group1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 route-map rmap2 in
```

#### Examples [BGP4+]

The following example shows the configuration of the route-map name **rmap2** and then the use of this map name in the **neighbor route-map** command for the neighbor with the IPv6 address 2001:0db8:010d::1 in the IPv6 Address Family Configuration mode.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 6
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1 route-map rmap2 in
```

The following example shows the removal of the route-map name **rmap2** in the **neighbor route-map** command for the neighbor with the IPv6 address 2001:0db8:010d::1 in the IPv6 Address Family Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1 route-map rmap2 in
```



The following example shows the configuration of the route-map name **rmap2** and then the use of this map name in the **neighbor route-map** command for the neighbor with the peer group named group1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 6
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 route-map rmap2 in
```

The following example shows the removal the route-map name **rmap2** in the **neighbor route-map** command for the neighbor with the peer group named group1 in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 route-map rmap2 in
```

**Related  
commands**

[address-family](#)  
[neighbor peer-group \(add a neighbor\)](#)  
[route-map](#)

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor route-reflector-client (BGP only)

**Overview** Use this command to configure the router as a BGP route reflector and configure the specified neighbor as its client.

Use the **no** variant of this command to indicate that the neighbor is not a client.

**Syntax** `neighbor <neighborid> route-reflector-client`  
`no neighbor <neighborid> route-reflector-client`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <peer-group> }                                                                                                                                                                                                                                                                                            |
| <ip-address> | The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                                   |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode** Router Configuration or IPv4 Address Family Configuration

**Usage notes** Route reflectors are a solution for the explosion of iBGP peering within an autonomous system. By route reflection the number of iBGP peers within an AS is reduced. Use the **neighbor route-reflector-client** command to configure the local router as the route reflector and specify neighbors as its client.

An AS can have more than one route reflector. One route reflector treats the other route reflector as another iBGP speaker.

In the following configuration, Router1 is the route reflector for clients 3 . 3 . 3 . 3 and 2 . 2 . 2 . 2; it also has a non-client peer 6 . 6 . 6 . 6:

```
Router1#
router bgp 200
neighbor 3.3.3.3 remote-as 200
neighbor 3.3.3.3 route-reflector-client
neighbor 2.2.2.2 remote-as 200
neighbor 2.2.2.2 route-reflector-client
neighbor 6.6.6.6 remote-as 200
```

**Examples**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72
route-reflector-client

awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72
route-reflector-client
```

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor route-server-client (BGP only)

**Overview** Use this command to specify the peer as route server client.  
Use the **no** variant of this command to disable this function.

**Syntax** `neighbor <neighborid> route-server-client`  
`no neighbor <neighborid> route-server-client`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | {<ip-address> <peer-group>}                                                                                                                                                                                                                                                                                                |
| <ip-address> | The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                                   |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode** Router Configuration

**Examples**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 route-server-client
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72
route-server-client
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor send-community

**Overview** Use this command to specify that a community attribute should be sent to a BGP or BGP4+ neighbor.

Use the **no** variant of this command to remove the entry for the community attribute.

**Syntax** `neighbor <neighborid> send-community {both|extended|standard}`  
`no neighbor <neighborid> send-community {both|extended|standard}`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                                                                   |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                                                                                 |
|              | <div><div>&lt;ip-address&gt;</div><div>Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.</div></div>                                                                                                                                                                                                                                           |
|              | <div><div>&lt;ipv6-addr&gt;</div><div>Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.</div></div>                                                                                                                                                                                                                               |
|              | <div><div>&lt;peer-group&gt;</div><div>Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group.</div></div> |
| both         | Sends Standard and Extended Community attributes. Specifying this parameter with the <b>no</b> variant of this command results in no standard or extended community attributes being sent.                                                                                                                                                                                    |
| extended     | Sends Extended Community attributes. Specifying this parameter with the <b>no</b> variant of this command results in no extended community attributes being sent.                                                                                                                                                                                                             |
| standard     | Sends Standard Community attributes. Specifying this parameter with the <b>no</b> variant of this command results in no standard community attributes being sent.                                                                                                                                                                                                             |

**Default** Both **standard** and **extended** community attributes are sent to a neighbor.

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration and IPv6 Address Family Configuration

**Usage notes** This command is used to specify a community attribute to be sent to a neighbor. The community attribute groups destinations in a certain community and applies routing decisions according to those communities. On receiving community attributes the router reannounces them to the neighbor. Only when the **no**

parameter is used with this command the community attributes are not reannounced to the neighbor.

By default, both **standard** and **extended** community attributes are sent to a neighbor.

### Examples [BGP]

```
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 send-community
extended

awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 send-community
extended

awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.0.72 send-community
extended

awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.0.72 send-community
extended

awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 send-community extended
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
send-community extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1
send-community extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
send-community extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
send-community extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 send-community extended
awplus# configure terminal
awplus(config)# bgp config-type standard
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 send-community
extended
```

**Related**  
**commands**

[bgp config-type](#)  
[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series



# neighbor shutdown

**Overview** Use this command to disable a peering relationship with a BGP or BGP4+ neighbor. Use the **no** variant of this command to re-enable the BGP or BGP4+ neighbor.

**Syntax** neighbor <neighborid> shutdown  
no neighbor <neighborid> shutdown

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <peer-group> }                                                                                                                                                                                                                                                                                            |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Usage notes** This command shuts down any active session for the specified BGP or BGP4+ neighbor and clears all related routing data.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.72 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.72 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 shutdown
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 shutdown
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 shutdown
```

**Related commands** [neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor soft-reconfiguration inbound

**Overview** Use this command to configure the device to start storing all updates from the BGP or BGP4+ neighbor, without any consideration of any inward route filtering policy that might be applied to the connection with this BGP or BGP4+ neighbor. This is so that the full set of the neighbor's updates are available locally to be used in a soft-reconfiguration event.

You may need to apply this older method of clearing routes if the peer does not support route refresh.

Use the **no** variant of this command to disable this function for a BGP or BGP4+ neighbor.

**Syntax** `neighbor <neighborid> soft-reconfiguration inbound`  
`no neighbor <neighborid> soft-reconfiguration inbound`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                              |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage** Use this command to store updates for inbound soft reconfiguration. Soft-reconfiguration may be used in lieu of BGP route refresh capability. Using this command enables local storage of all the received routes and their attributes. This requires additional memory. When a soft reset (inbound) is done on this neighbor, the locally stored routes are re-processed according to the inbound policy. The BGP neighbor connection is not affected.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# neighbor 10.10.10.10
soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor 10.10.10.10
soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.10 soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.10 soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 soft-reconfiguration
inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# no neighbor group1 soft-reconfiguration
inbound
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
soft-reconfiguration inbound
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 soft-reconfiguration
inbound
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)# address-family ipv6
awplus(config-router-
af)# no neighbor group1 soft-reconfiguration inbound
```

**Related**  
**commands**

[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor timers

**Overview** Use this command to set the keepalive, holdtime, and connect timers for a specific BGP or BGP4+ neighbor.

Use the **no** variant of this command to clear the timers for a specific BGP or BGP4+ neighbor.

**Syntax** `neighbor <neighborid> timers {<keepalive> <holdtime>|connect <connect>}`  
`no neighbor <neighborid> timers [connect]`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | {<ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                                            |
|              | <ip-address> Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
|              | <ipv6-addr> Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                               |
|              | <peer-group> Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <keepalive>  | <0-65535> Frequency (in seconds) at which a router sends keepalive messages to its neighbor.                                                                                                                                                                                                                                            |
| <holdtime>   | <0-65535> Interval (in seconds) after which, on not receiving a keepalive message, the router declares a neighbor dead.                                                                                                                                                                                                                 |
| <connect>    | <code>connect &lt;1-65535&gt;</code> Specifies the connect timer in seconds. The default connect timer value is 120 seconds as per RFC 4271. Modify this value as needed for interoperability.                                                                                                                                          |

**Default** The keepalive timer default is 60 seconds, the holdtime timer default is 90 seconds, and the connect timer default is 120 seconds as per RFC 4271. Holdtime is keepalive \* 3.

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Usage** Keepalive messages are sent by a router to inform another router that the BGP connection between the two is still active. The keepalive interval is the period of time between each keepalive message sent by the router. The holdtime interval is the time the router waits to receive a keepalive message and if it does not receive

a message for this period it declares the neighbor dead. The holdtime value must be 3 times the value of the keepalive value.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 timers 60 120
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 timers
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 timers 60 120
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 timers
```

**Examples [BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1 timers 60 120
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 2001:0db8:010d::1 timers
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 timers 60 120
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 timers
```

**Related commands**   neighbor peer-group (add a neighbor)  
neighbor route-map  
show ip bgp neighbors hold-time (BGP only)  
show ip bgp neighbors keepalive-interval (BGP only)  
timers (BGP)

**Command changes**   Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# neighbor transparent-as

**Overview** Use this command to specify not to append your AS path number even if the BGP or BGP4+ peer is an eBGP peer.

Note this command has the same effect as invoking [neighbor attribute-unchanged](#) and specifying the optional **as-path** parameter.

**Syntax** neighbor <neighborid> transparent-as

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                              |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode** Router Configuration

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 transparent-as
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 transparent-as
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
transparent-as
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 transparent-as
```

**Related**  
**commands**

[neighbor attribute-unchanged](#)  
[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)  
[neighbor transparent-nexthop](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor transparent-nexthop

**Overview** Use this command to keep the next hop value of the route even if the BGP or BGP4+ peer is an eBGP peer.

Note this command has the same effect as invoking [neighbor attribute-unchanged](#) and specifying the optional **next-hop** parameter.

**Syntax** `neighbor <neighborid> transparent-nexthop`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | {<ip-address>   <ipv6-addr>   <peer-group>}                                                                                                                                                                                                                                                                                |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |

**Mode** Router Configuration

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 transparent-nexthop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 transparent-nexthop
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 2001:0db8:010d::1
transparent-nexthop
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 transparent-nexthop
```

**Related**  
**commands**

[neighbor attribute-unchanged](#)  
[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)  
[neighbor transparent-as](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor unsuppress-map

**Overview** Use this command to selectively leak more specific routes to a particular BGP or BGP4+ neighbor.

Use the **no** variant of this command to remove selectively leaked specific routes to a particular BGP or BGP4+ neighbor.

**Syntax** `neighbor <neighborid> unsuppress-map <route-map-name>`  
`no neighbor <neighborid> unsuppress-map <route-map-name>`

| Parameter        | Description                                                                                                                                                                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid>     | { <ip-address>   <ipv6-addr>   <peer-group> }                                                                                                                                                                                                                                                                              |
| <ip-address>     | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>      | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group>     | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <route-map-name> | The name of the route-map used to select routes to be unsuppressed.                                                                                                                                                                                                                                                        |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage** When the [aggregate-address](#) command is used with the **summary-only** option, the more-specific routes of the aggregate are suppressed to all neighbors. Use this command instead to selectively leak more-specific routes to a particular neighbor.

**Examples [BGP]** To allow the device to advertise specific routes in the routemap 'mymap', which would have otherwise been aggregated to neighbor 10.10.0.73, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.0.73 unsuppress-map mymap
```

To stop the device from advertising specific routes in the routemap, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.0.73 unsuppress-map mymap
```

To allow the device to advertise specific IPv4 routes in the routemap 'mymap', which would have otherwise been aggregated to neighbor 10.10.0.73, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4 unicast
awplus(config-router-af)# neighbor 10.10.0.70 unsuppress-map mymap
```

To stop the device from advertising specific IPv4 routes in the routemap, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4 unicast
awplus(config-router-af)# no neighbor 10.10.0.70 unsuppress-map mymap
```

To allow the device to advertise specific routes in the routemap 'mymap', which would have otherwise been aggregated to peer group 'group1', use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 unsuppress-map mymap
```

To stop the device from advertising specific routes in the routemap to peer group 'group1', use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 unsuppress-map mymap
```

**Examples**  
**[BGP4+]** To allow the device to advertise specific IPv6 routes in the routemap 'mymap', which would have otherwise been aggregated to neighbor 2001:0db8:010d::1, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6 unicast
awplus(config-router-af)# neighbor 2001:0db8:010d::1
unsuppress-map mymap
```

To stop the device from advertising specific IPv6 routes in the routemap, use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6 unicast
awplus(config-router-af)# no neighbor 2001:0db8:010d::1
unsuppress-map mymap
```

To allow the device to advertise specific IPv6 routes in the routemap 'mymap', which would have otherwise been aggregated to peer group 'group1', use the commands

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 unsuppress-map mymap
```

To stop the device from advertising specific IPv6 routes in the routemap to peer group 'group1', use the commands:

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 unsuppress-map
mymap
```

**Related commands**

- [aggregate-address](#)
- [neighbor peer-group \(add a neighbor\)](#)
- [neighbor route-map](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor update-source

**Overview** Use this command to specify the source IPv4 or IPv6 address of BGP or BGP4+ packets, which are sent to the neighbor for routing updates, as the IPv4 or IPv6 address configured on the specified interface. The specified interface is usually the local loopback (lo) interface to allow internal BGP or BGP4+ connections to stay up regardless of which interface is used to reach a neighbor.

Use the **no** variant of this command to remove the IPv4 or IPv6 address from the interface as the source IPv4 or IPv6 address of BGP or BGP4+ packets sent to the neighbor, and restores the interface assignment to the closest interface, which is also called the best local address.

**Syntax** `neighbor <neighborid> update-source <interface>`  
`no neighbor <neighborid> update-source`

| Parameter                       | Description                                                                                                                                                                                                                                                                                                                |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;neighborid&gt;</code> | { <code>&lt;ip-address&gt;</code>   <code>&lt;ipv6-addr&gt;</code>   <code>&lt;peer-group&gt;</code> }                                                                                                                                                                                                                     |
| <code>&lt;ip-address&gt;</code> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <code>&lt;ipv6-addr&gt;</code>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <code>&lt;peer-group&gt;</code> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <code>&lt;interface&gt;</code>  | Specifies the local loopback interface (lo).                                                                                                                                                                                                                                                                               |

**Default** Use of this command sets a default value of 2 for the maximum hop count.

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration

**Usage** Use this command in conjunction with any specified interface on the router. The local loopback interface is the interface that is most commonly used with this command. The use of local loopback interface eliminates a dependency and BGP or BGP4+ does not have to rely on the availability of a particular interface for making BGP or BGP4+ peer relationships.



**Examples [BGP]** To source BGP connections for neighbor 10.10.0.72 with the IP address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.0.73/24
awplus(config-if)# exit
awplus(config)# router bgp 100
awplus(config-router)# network 10.10.0.0
awplus(config-router)# neighbor 10.10.0.72 remote-as 110
awplus(config-router)# neighbor 10.10.0.72 update-source lo
```

To remove BGP connections for neighbor 10.10.0.72 with the IP address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# router bgp 100
awplus(config-router)# no neighbor 10.10.0.72 update-source
```

To source BGP connections for neighbor group1 with the IP address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.0.73/24
awplus(config-if)# exit
awplus(config)# router bgp 100
awplus(config-router)# network 10.10.0.0
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.0.72 remote-as 100
awplus(config-router)# neighbor 10.10.0.72 peer-group group1
awplus(config-router)# neighbor group1 update-source lo
```

To remove BGP connections for neighbor group1 with the IP address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# router bgp 100
awplus(config-router)# neighbor group1 update-source lo
```

**Examples** To source BGP connections for neighbor 2001:0db8:010d::1 with the IPv6 address  
**[BGP4+]** of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# interface lo
awplus(config-if)# ipv6 address 2001:0db8:010d::1/128
awplus(config-if)# exit
awplus(config)# router bgp 100
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 110
awplus(config-router)# neighbor 2001:0db8:010d::1
update-source lo
```

To remove BGP connections for neighbor 2001:0db8:010d::1 with the IPv6 address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# router bgp 100
awplus(config-router)# no neighbor 2001:0db8:010d::1
update-source
```

To source BGP connections for neighbor group1 with the IPv6 address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# interface lo
awplus(config-if)# ipv6 address 2001:0db8:010d::1/128
awplus(config-if)# exit
awplus(config)# router bgp 100
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1 peer-group group1
awplus(config-router-af)# exit
awplus(config-router)# neighbor group1 update-source lo
```

To remove BGP connections for neighbor group1 with the IPv6 address of the local loopback address instead of the best local address, enter the commands listed below:

```
awplus(config)# router bgp 100
awplus(config-router)# neighbor group1 update-source lo
```

**Related commands** [neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series

## Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor version (BGP only)

**Overview** Use this command to configure the device to accept only a particular BGP version.  
Use the **no** variant of this command to use the default BGP version (version 4).

**Syntax** `neighbor <neighborid> version <version>`  
`no neighbor <neighborid> version`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                             |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | { <ip-address>   <peer-group> }                                                                                                                                                                                                                                                                                                         |
|              | <ip-address> The address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                                   |
|              | <peer-group> Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <version>    | {4} Specifies the BGP version number.                                                                                                                                                                                                                                                                                                   |

**Mode** Router Configuration or IPv4 Address Family Configuration

**Usage notes** By default, the system uses BGP version 4 and on request dynamically negotiates down to version 2. Using this command disables the router's version-negotiation capability and forces the router to use only a specified version with the neighbor.

**Examples**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 version 4
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 version 4
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 version
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 version
```

**Related commands** [neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# neighbor weight

**Overview** Use this command to set default weights for routes from this BGP or BGP4+ neighbor.

Use the **no** variant of this command to remove a weight assignment.

**Syntax** `neighbor <neighborid> weight <weight>`  
`no neighbor <neighborid> weight [<weight>]`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <neighborid> | {<ip-address> <ipv6-addr> <peer-group>}                                                                                                                                                                                                                                                                                    |
| <ip-address> | Specify the address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                           |
| <ipv6-addr>  | Specify the address of an IPv6 BGP4+ neighbor, entered in hexadecimal in the format X:X::X:X.                                                                                                                                                                                                                              |
| <peer-group> | Enter the name of an existing peer-group. For information on how to create peer groups, refer to the <a href="#">neighbor peer-group (add a neighbor)</a> command, and <a href="#">neighbor route-map</a> command. When this parameter is used with this command, the command applies on all peers in the specified group. |
| <weight>     | <0-65535> Specifies the weight this command assigns to the route.                                                                                                                                                                                                                                                          |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage notes** Use this command to specify a weight value to all routes learned from a BGP or BGP4+ neighbor. The route with the highest weight gets preference when there are other routes on the network.

Unlike the local-preference attribute, the weight attribute is relevant only to the local router.

The weights assigned using the **set weight** command overrides the weights assigned using this command.

**Examples [BGP]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor 10.10.10.1 weight 60
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor 10.10.10.1 weight
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# neighbor 10.10.10.1 weight 60
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv4
awplus(config-router-af)# no neighbor 10.10.10.1 weight
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 10.10.10.1 remote-as 10
awplus(config-router)# neighbor 10.10.10.1 peer-group group1
awplus(config-router)# neighbor group1 weight 60
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no neighbor group1 weight
```

**Examples**  
**[BGP4+]**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1 weight 60
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor 2001:0db8:010d::1 weight
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# neighbor group1 peer-group
awplus(config-router)# neighbor 2001:0db8:010d::1 remote-as 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# neighbor 2001:0db8:010d::1
peer-group group1
awplus(config-router-af)# neighbor group1 weight 60
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# address-family ipv6
awplus(config-router-af)# no neighbor group1 weight
```

**Related**  
**commands**

[neighbor peer-group \(add a neighbor\)](#)  
[neighbor route-map](#)

**Command**  
**changes**

Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# network (BGP and BGP4+)

**Overview** Use this command to specify particular routes to be advertised into the BGP or BGP4+ routing process. A unicast network address without a mask is accepted if it falls into the natural boundary of its class. A class-boundary mask is derived if the address matches its natural class-boundary.

Note that you can specify a prefix length for the prefix being added, and you can also specify a classful network without a prefix length and an appropriate prefix length is added. Note that specifying a non-classful prefix without a prefix length results in a /32 prefix length on an IPv4 route.

Use the **no** variant of this command to remove a network route entry.

**Syntax [BGP]** `network {<ip-prefix/length>|<ip-network-addr>} [mask <network-mask>] [route-map <route-map-name>] [backdoor]`  
`no network {<ip-prefix/length>|<ip-network-addr>} [mask <network-mask>] [route-map <route-map-name>] [backdoor]`

**Syntax [BGP4+]** `network {<ipv6-prefix/length>|<ipv6-network-addr>} [route-map <route-map-name>]`  
`no network {<ipv6-prefix/length>|<ipv6-network-addr>} [route-map <route-map-name>]`

| Parameter            | Description                                                                                                                                                                                     |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-prefix/length>   | IP network prefix and prefix length entered in dotted decimal format for the IP network prefix, then slash notation for the prefix length in the format A.B.C.D/M, e.g. 192.168.1.224/27        |
| <ip-network-addr>    | IP network prefix entered in dotted decimal format A.B.C.D, e.g. 192.168.1.224                                                                                                                  |
| <network-mask>       | Specify a network mask in the format A.B.C.D, e.g. 255.255.255.224.                                                                                                                             |
| <ipv6-prefix/length> | IPv6 network prefix and prefix length entered in dotted decimal format for the IPv6 network prefix, then slash notation for the IPv6 prefix length in the format X:X::X:X/M, e.g. 2001:db8::/64 |
| <ipv6-network-addr>  | IP network prefix entered in dotted decimal format A.B.C.D, e.g. 192.168.1.224                                                                                                                  |
| <route-map-name>     | Specify the name of the route map.                                                                                                                                                              |
| backdoor             | Specify a BGP backdoor route that is not advertised.                                                                                                                                            |

**Mode [BGP]** Router Configuration and IPv4 Address Family [ipv4 unicast] mode

**Mode [BGP4+]** IPv6 Address Family Configuration

**Usage notes** It does not matter how the route is arranged in the IP or IPv6 routing table. The route can arrive in the IP routing table by a static route, or the route can be learned from OSPF or OSPFv3 or RIP or RIPng routing.

If you configure a route-map, then that route-map will be used in filtering the network, or the route-map will be used to modify the attributes that are advertised with the route.

**Example [BGP]** The following example illustrates a Class-A address configured as a network route. The natural Class-A network prefix mask length of 8 will be internally derived, that is, 2.0.0.0/8.

```
awplus(config)# router bgp 100
awplus(config-router)# network 2.0.0.0
```

**Output [BGP]** Figure 24-1: Example output from the **show running-config** command after entering **network 2.0.0.0**

```
awplus#show running-config

router bgp 100
 network 2.0.0.0/8
```

**Example [BGP]** The following example illustrates a network address which does not fall into its natural class boundary, and hence, is perceived as a host route, that is, 192.0.2.224/27.

```
awplus(config)# router bgp 100
awplus(config-router)# network 192.0.2.224 mask 255.255.255.224
```

**Output [BGP]** Figure 24-2: Example output from the **show running-config** command after entering **network 192.0.2.224 mask 255.255.255.224**

```
awplus#show running-config

router bgp 100
 network 192.0.2.224/27
```

**Example [BGP]** The following example is the same as the previous example for host route 192.0.2.224/27, but is entered in prefix/length format using slash notation (instead of prefix plus mask in dotted decimal format using the **mask** keyword before the network mask in dotted decimal format):

```
awplus(config)# router bgp 100
awplus(config-router)# network 192.0.2.224/27
```

**Example [BGP4+]** The following example is the same as the previous example for host route 2001:db8::/32:

```
awplus(config)# router bgp 100
awplus(config-router)# address-family ipv6
awplus(config-router-af)# network 2001:db8::/32
```

**Output [BGP4+]** Figure 24-3: Example output from the **show running-config** command after entering **network 2001:db8::/32**

```
awplus#show running-config

router bgp 100
 network 2001:db8::/32
```

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# network synchronization

**Overview** Use this command to ensure the exact same static network prefix, specified through any of the **network** commands, is local or has IGP reachability before introduction to BGP or BGP4+.

Use the **no** variant of this command to disable this function.

**Syntax** `network synchronization`  
`no network synchronization`

**Default** Network synchronization is disabled by default.

**Mode [BGP]** Router Configuration and IPv4 Address Family [ipv4 unicast] Configuration

**Mode [BGP4+]** IPv6 Address Family [ipv6 unicast] Configuration

**Examples [BGP]** The following example enables IGP synchronization of BGP static network routes in the Router Configuration mode.

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# network synchronization
```

The following example enables IGP synchronization of BGP static network routes in the IPv4-Unicast address family.

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# address-family ipv4 unicast
awplus(config-router-af)# network synchronization
```

**Example [BGP4+]** The following example enables IGP synchronization of BGP4+ static network routes in the IPv6-Unicast address family.

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# address-family ipv6 unicast
awplus(config-router-af)# network synchronization
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# redistribute (into BGP or BGP4+)

**Overview** Use this command to inject routes from one routing process into a BGP or BGP4+ routing table.

Use the **no** variant of this command to disable this function.

**Syntax** `redistribute {ospf|rip|connected|static} [route-map  
<route-map-entry-pointer>]`  
`no redistribute {ospf|rip|connected|static} [route-map  
<route-map-entry-pointer>]`

| Parameter                 | Description                                                                               |
|---------------------------|-------------------------------------------------------------------------------------------|
| connected                 | Specifies the redistribution of connected routes for both BGP and BGP4+.                  |
| ospf                      | Specifies the redistribution of OSPF information for BGP or OSPFv3 information for BGP4+. |
| rip                       | Specifies the redistribution of RIP information for BGP or RIPng information for BGP4+.   |
| static                    | Specifies the redistribution of Static routes for both BGP and BGP4+.                     |
| route-map                 | Route map reference for both BGP and BGP4+.                                               |
| <route-map-entry-pointer> | Pointer to route-map entries.                                                             |

**Mode [BGP]** Router Configuration or IPv4 Address Family Configuration

**Mode [BGP4+]** Router Configuration or IPv6 Address Family Configuration

**Usage notes** Redistribution is used by routing protocols to advertise routes that are learned by some other means, such as by another routing protocol or by static routes. Since all internal routes are dumped into BGP, careful filtering is applied to make sure that only routes to be advertised reach the internet, not everything. This command allows redistribution by injecting prefixes from one routing protocol into another routing protocol.

**Examples [BGP/ BGP+]** The following example shows the configuration of a route-map named `rmap1`, which is then applied using the **redistribute route-map** command.

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 1
awplus(config-route-map)# match origin incomplete
awplus(config-route-map)# set metric 100
awplus(config-route-map)# exit
awplus(config)# router bgp 12
awplus(config-router)# redistribute ospf route-map rmap1
```

The following example shows the configuration of a route-map named `rmap2`, which is then applied using the **redistribute route-map** command.

```
awplus# configure terminal
awplus(config)# route-map rmap2 permit 3
awplus(config-route-map)# match interface eth1
awplus(config-route-map)# set metric-type 1
awplus(config-route-map)# exit
awplus(config)# router ospf 100
awplus(config-router)# redistribute bgp route-map rmap2
```

Note that configuring a route-map and applying it with the **redistribute route-map** command allows you to filter which routes are distributed from another routing protocol (such as OSPF with BGP). A route-map can also set the metric, tag, and metric-type of the redistributed routes.

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

## restart bgp graceful (BGP only)

**Overview** Use this command to force the device to perform a graceful BGP restart.

**Syntax** `restart bgp graceful`

**Mode** Privileged Exec

**Usage** Before using this command, BGP graceful-restart capabilities must be enabled within the router BGP ([bgp graceful-restart](#) command), and each neighbor configured on the device should be set to advertise its graceful-restart capability ([bgp graceful-restart graceful-reset](#) command). The neighbor devices also need to have BGP graceful-restart capabilities enabled ([bgp graceful-restart](#) command).

This command stops the whole BGP process and makes the device retain the BGP routes and mark them as stale. Receiving BGP speakers, retain and mark as stale all BGP routes received from the restarting speaker for all the address families received in the Graceful Restart Capability exchange.

When a **restart bgp graceful** command is issued, the BGP configuration is reloaded from the last saved configuration. Ensure you first issue a **copy running-config startup-config**.

**Example** `awplus# restart bgp graceful`

**Related commands** [bgp graceful-restart](#)  
[bgp graceful-restart graceful-reset](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# router bgp

**Overview** Use this command to configure a BGP routing process, specifying the 32-bit Autonomous System (AS) number.

Use the **no** variant of this command to disable a BGP routing process, specifying the 32-bit AS number.

**Syntax** router bgp <asn>  
no router bgp <asn>

| Parameter | Description                                                        |
|-----------|--------------------------------------------------------------------|
| <asn>     | <1-4294967295> Specifies the 32-bit Autonomous System (AS) number. |

**Mode** Global Configuration

**Usage** The **router bgp** command enables a BGP routing process:

```
router bgp 1
 neighbor 10.0.0.1 remote-as 1
 neighbor 10.0.0.2 remote-as 1
 !
router bgp 2
 neighbor 10.0.0.3 remote-as 2
 neighbor 10.0.0.4 remote-as 2
```

**Examples**

```
awplus# configure terminal
awplus(config)# router bgp 12
awplus(config-router)#
awplus# configure terminal
awplus(config)# no router bgp 12
awplus(config)#
```

**Command changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series



# route-map

**Overview** Use this command to configure a route map entry, and to specify whether the device will process or discard matching routes and BGP update messages.

The device uses a name to identify the route map, and a sequence number to identify each entry in the route map.

The **route-map** command puts you into route-map configuration mode. In this mode, you can use the following:

- one or more of the **match** commands to create match clauses. These specify what routes or update messages match the entry.
- one or more of the **set** commands to create set clauses. These change the attributes of matching routes or update messages.

Use the **no** variant of this command to delete a route map or to delete an entry from a route map.

**Syntax** `route-map <mapname> {deny|permit} <seq>`  
`no route-map <mapname>`  
`no route-map <mapname> {deny|permit} <seq>`

| Parameter | Description                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------|
| <mapname> | A name to identify the route map.                                                                                         |
| deny      | The route map causes a routing process to discard matching routes or BGP update messages.                                 |
| permit    | The route map causes a routing process to use matching routes or BGP update messages.                                     |
| <seq>     | <1-65535> The sequence number of the entry. You can use this parameter to control the order of entries in this route map. |

**Mode** Global Configuration

**Usage notes** Route maps allow you to control and modify routing information by filtering routes and setting route attributes. You can apply route maps when the device:

- processes BGP update messages that it has received from a peer
- prepares BGP update messages to send to peers
- redistributes routes from one routing protocol into another
- redistributes static routes into routing protocols
- uses BGP route flap dampening

When a routing protocol passes a route or update message through a route map, it checks the entries in order of their sequence numbers, starting with the lowest numbered entry.

If it finds a match on a route map with an action of permit, then it applies any set clauses and accepts the route. Having found a match, the route is not compared against any further entries of the route map.

If it finds a match on a route map with an action of deny, it will discard the matching route.

If it does not find a match, it discards the route or update message. This means that route maps end with an implicit deny entry. To permit all non-matching routes or update messages, end your route map with an entry that has an action of **permit** and no match clause.

**Examples** To enter route-map mode for entry 1 of the route map called "route1", and then add a match and set clause to it, use the commands:

```
awplus# configure terminal
awplus(config)# route-map route1 permit 1
awplus(config-route-map)# match as-path 60
awplus(config-route-map)# set weight 70
```

To enter route-map mode for entry 2 of the route map called "route1", and then add a match and set clause to it, use the commands:

```
awplus# configure terminal
awplus(config)# route-map route1 permit 2
awplus(config-route-map)# match interface eth1
awplus(config-route-map)# set metric 20
```

Note how the prompt changes when you go into route map configuration mode.

To make the device process non-matching routes instead of discarding them, add a command like the following one:

```
awplus(config)# route-map route1 permit 100
```

**Related  
commands**

For BGP:

- [show route-map](#)
- [bgp dampening](#)
- [neighbor default-originate](#)
- [neighbor route-map](#)
- [neighbor unsuppress-map](#)
- [network \(BGP and BGP4+\)](#)
- [redistribute \(into BGP or BGP4+\)](#)
- [show ip bgp route-map \(BGP only\)](#)

For OSPF:

- [default-information originate](#)
- [redistribute \(OSPF\)](#)

For RIP:

`redistribute (RIP)`

# set as-path

**Overview** Use this command to add an AS path set clause to a route map entry.

When a BGP update message matches the route map entry, the device prepends the specified Autonomous System Number (ASN) or ASNs to the update's AS path attribute.

The AS path attribute is a list of the autonomous systems through which the announcement for the prefix has passed. As prefixes pass between autonomous systems, each autonomous system adds its ASN to the beginning of the list. This means that the AS path attribute can be used to make routing decisions.

Use the **no** variant of this command to remove the set clause.

**Syntax** `set as-path prepend <1-65535> [<1-65535>]...`  
`no set as-path prepend [<1-65535> [<1-65535>]...]`

| Parameter                    | Description                                                                                    |
|------------------------------|------------------------------------------------------------------------------------------------|
| <code>prepend</code>         | Prepends the autonomous system path.                                                           |
| <code>&lt;1-65535&gt;</code> | The number to prepend to the AS path. If you specify multiple ASNs, separate them with spaces. |

**Mode** Route-map mode

**Usage notes** Use the **set as-path** command to specify an autonomous system path. By specifying the length of the AS-Path, the device influences the best path selection by a neighbor. Use the `prepend` parameter with this command to prepend an AS path string to routes increasing the AS path length.

This command is valid for BGP update messages only.

**Example** To use entry 3 of the route map called `myroute` to prepend ASN 8 and 24 to the AS path of matching update messages, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# set as-path prepend 8 24
```

**Related commands** [match as-path](#)  
[route-map](#)  
[show route-map](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# set community

**Overview** Use this command to add a community set clause to a route map entry.

When a BGP update message matches the route map entry, the device takes one of the following actions:

- changes the update's community attribute to the specified value or values, or
- adds the specified community value or values to the update's community attribute, if you specify the **additive** parameter after specifying another parameter. or
- removes the community attribute from the update, if you specify the **none** parameter

Use the **no** variant of this command to remove the set clause.

**Syntax**

```
set community {[<1-65535>][AA:NN] [internet] [local-AS]
[no-advertise] [no-export] [additive]}

no set community {[AA:NN] [internet] [local-AS] [no-advertise]
[no-export] [additive]}

set community none

no set community none
```

| Parameter    | Description                                                                                                                                                                                                                                                                                                                                                         |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-65535>    | The AS number of the community as an integer not in AA:NN format.                                                                                                                                                                                                                                                                                                   |
| AA:NN        | The Autonomous System (AS) number of the community, in AA:NN format. AS numbers are assigned to the regional registries by the IANA ( <a href="http://www.iana.org">www.iana.org</a> ) and can be obtained from the registry in your region.<br>AA and NN are both integers from 1 to 65535.<br>AA is the AS number; NN is a value chosen by the ASN administrator. |
| local-AS     | The community of routes that must not be advertised to external BGP peers (this includes peers in other members' Autonomous Systems inside a BGP confederation).                                                                                                                                                                                                    |
| internet     | The community of routes that can be advertised to all BGP peers.                                                                                                                                                                                                                                                                                                    |
| no-advertise | The community of routes that must not be advertised to other BGP peers.                                                                                                                                                                                                                                                                                             |
| no-export    | The community of routes that must not be advertised outside a BGP confederation boundary (a standalone Autonomous System that is not part of a confederation should be considered a confederation itself).                                                                                                                                                          |

| Parameter | Description                                                                                                                                                                                                                       |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| none      | The device removes the community attribute from matching update messages.                                                                                                                                                         |
| additive  | The device adds the specified community value to the update message's community attribute, instead of replacing the existing attribute. By default this parameter is not included, so the device replaces the existing attribute. |

**Mode** Route-map Configuration

**Usage notes** This command is valid for BGP update messages only.

**Examples** To use entry 3 of the route map called `rmap1` to put matching routes into the no-advertise community, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community no-advertise
```

To use entry 3 of the route map called `rmap1` to put matching routes into several communities, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community 10:01 23:34 12:14
no-export
```

To use entry 3 of the route map called `rmap1` to put matching routes into a single AS community numbered 16384, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community 16384 no-export
```

**Related commands**

- [match community](#)
- [route-map](#)
- [set aggregator](#)
- [set comm-list delete](#)
- [set extcommunity](#)
- [show route-map](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

## show bgp ipv6 (BGP4+ only)

**Overview** Use this command to display BGP4+ network information for a specified IPv6 address.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 <ipv6-addr>`

| Parameter                      | Description                                                                |
|--------------------------------|----------------------------------------------------------------------------|
| <code>&lt;ipv6-addr&gt;</code> | Specifies the IPv6 address, entered in hexadecimal in the format X:X::X:X. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show bgp ipv6 2001:0db8:010d::1`

**Related commands** [show bgp ipv6 longer-prefixes \(BGP4+ only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp ipv6 community (BGP4+ only)

**Overview** Use this command to display routes that match specified communities within an IPv6 environment. Use the [show ip bgp community \(BGP only\)](#) command within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

You may use any combination and repetition of parameters listed in the *<type>* placeholder.

**Syntax** `show bgp ipv6 community [<type>] [exact-match]`

| Parameter           | Description                                                                                                 |
|---------------------|-------------------------------------------------------------------------------------------------------------|
| <i>&lt;type&gt;</i> | {[ <i>AA:NN</i> ] [ <i>local-AS</i> ] [ <i>no-advertise</i> ] [ <i>no-export</i> ] }                        |
| <i>AA:NN</i>        | Specifies the Autonomous System (AS) community number, in AA:NN format.                                     |
| <i>local-AS</i>     | Do not send outside local Autonomous Systems (well-known community).                                        |
| <i>no-advertise</i> | Do not advertise to any peer (well-known community).                                                        |
| <i>no-export</i>    | Do not export to next AS (well-known community).                                                            |
| <i>exact-match</i>  | Specifies that the exact match of the communities is displayed. This optional parameter cannot be repeated. |

**Mode** User Exec and Privileged Exec

**Examples** Note that the AS numbers shown are examples only.

```
awplus# show bgp ipv6 community 64497:64499 exact-match
awplus# show bgp ipv6 community 64497:64499 64500:64501
exact-match
awplus# show bgp ipv6 community 64497:64499 64500:64501
64510:64511no-advertise
awplus# show bgp ipv6 community no-advertise
no-advertiseno-advertise exact-match
awplus# show bgp ipv6 community no-export 64510:64511
no-advertise local-AS no-export
awplus# show bgp ipv6 community no-export 64510:64511
no-advertise 64497:64499 64500:64501 no-export
awplus# show bgp ipv6 community no-export 64497:64499
no-advertise local-AS no-export
```



**Related commands** [show ip bgp community \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp ipv6 community-list (BGP4+ only)

**Overview** Use this command to display routes that match the given community-list within an IPv6 environment. Use the [show ip bgp community-list \(BGP only\)](#) command within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 community-list <listname> [exact-match]`

| Parameter   | Description                                                            |
|-------------|------------------------------------------------------------------------|
| <listname>  | Specifies the community list name.                                     |
| exact-match | Displays only routes that have exactly the same specified communities. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show bgp ipv6 community-list mylist exact-match`

**Related commands** [show ip bgp community-list \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp ipv6 dampening (BGP4+ only)

**Overview** Use this command to show dampened routes from a BGP4+ instance within an IPv6 environment. Use the [show ip bgp dampening \(BGP only\)](#) command to show dampened routes from a BGP instance within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 dampening  
{dampened-paths|flap-statistics|parameters}`

| Parameter       | Description                                         |
|-----------------|-----------------------------------------------------|
| dampened-paths  | Display paths suppressed due to dampening.          |
| flap-statistics | Display flap statistics of routes.                  |
| parameters      | Display details of configured dampening parameters. |

**Mode** User Exec and Privileged Exec

**Usage notes** Enable BGP4+ dampening to maintain dampened-path information in memory.

**Examples**

```
awplus# show bgp ipv6 dampening dampened-path
awplus# show bgp ipv6 dampening flap-statistics
awplus# show bgp ipv6 dampening parameter
```

**Related commands** [show ip bgp dampening \(BGP only\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp ipv6 filter-list (BGP4+ only)

**Overview** Use this command to display routes conforming to the filter-list within an IPv6 environment. Use the [show ip bgp filter-list \(BGP only\)](#) command to display routes conforming to the filter-list within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 filter-list <listname>`

| Parameter  | Description                                        |
|------------|----------------------------------------------------|
| <listname> | Specifies the regular-expression access list name. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show bgp ipv6 filter-list mylist`

**Related commands** [show ip bgp filter-list \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp ipv6 inconsistent-as (BGP4+ only)

**Overview** Use this command to display routes with inconsistent AS Paths within an IPv6 environment. Use the [show ip bgp inconsistent-as \(BGP only\)](#) command to display routes with inconsistent AS paths within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 inconsistent-as`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show bgp ipv6 inconsistent-as`

**Related commands** [show ip bgp inconsistent-as \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp ipv6 longer-prefixes (BGP4+ only)

**Overview** Use this command to display the route of the local BGP4+ routing table for a specific prefix with a specific mask or for any prefix having a longer mask than the one specified.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 <ipv6-addr/prefix-length> longer-prefixes`

| Parameter                                    | Description                                                                                                                                                |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-addr/prefix-length&gt;</code> | Specifies the IPv6 address with prefix length. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show bgp ipv6 2001:0db8::/64 longer-prefixes`

**Related commands** [show bgp ipv6 \(BGP4+ only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp ipv6 neighbors (BGP4+ only)

**Overview** Use this command to display detailed information on peering connections to all BGP4+ neighbors within an IPv6 environment.

Use the [show ip bgp neighbors \(BGP only\)](#) command to display detailed information on peering connections to all BGP neighbors within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 neighbors [<ipv6-addr> [advertised-routes|received prefix-filter|received-routes|routes]]`

| Parameter              | Description                                                                                                                                       |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv6-addr>            | Specifies the IPv6 address, entered in hexadecimal in the format X:X::X:X.                                                                        |
| advertised-routes      | Displays the routes advertised to a BGP4+ neighbor.                                                                                               |
| received prefix-filter | Displays received prefix-list filters.                                                                                                            |
| received-routes        | Displays the received routes from the neighbor. To display all the received routes from the neighbor, configure the BGP4+ soft reconfigure first. |
| routes                 | Displays all accepted routes learned from neighbors.                                                                                              |

**Mode** User Exec and Privileged Exec

**Examples**  
**[BGP4+]**

```
awplus# show bgp ipv6 neighbors 2001:0db8:010d::1
advertised-routes

awplus# show bgp ipv6 neighbors 2001:0db8:010d::1 received
prefix-filter

awplus# show bgp ipv6 neighbors 2001:0db8:010d::1
received-routes

awplus# show bgp ipv6 neighbors 2001:0db8:010d::1 routes
```

**Output** Figure 24-4: Example output from **show bgp ipv6 neighbors 2001:db8:b::1**

```
awplus#show bgp ipv6 neighbors 2001:db8:b::1
BGP neighbor is 2001:db8:b::1, remote AS 200, local AS 100, external link
 BGP version 4, remote router ID 2.2.2.1
 BGP state = Established, up for 01:03:26
 Last read 01:03:26, hold time is 90, keepalive interval is 30 seconds
 Neighbor capabilities:
 Route refresh: advertised and received (old and new)
 4-Octet ASN Capability: advertised and received
 Address family IPv4 Unicast: advertised and received
 Address family IPv6 Unicast: advertised and received
 Received 157 messages, 0 notifications, 0 in queue
 Sent 228 messages, 0 notifications, 0 in queue
 Route refresh request: received 0, sent 0
 Minimum time between advertisement runs is 30 seconds
 Update source is lo
For address family: IPv4 Unicast
 BGP table version 1, neighbor version 1
 Index 2, Offset 0, Mask 0x4
 Community attribute sent to this neighbor (both)
 0 accepted prefixes
 0 announced prefixes

For address family: IPv6 Unicast
 BGP table version 66, neighbor version 66
 Index 2, Offset 0, Mask 0x4
 AF-dependant capabilities:
 Graceful restart: advertised, received

 Community attribute sent to this neighbor (both)
 Default information originate, default sent
 Inbound path policy configured
 Incoming update prefix filter list is *BGP_FILTER_LIST
 Route map for incoming advertisements is *BGP_LOCAL_PREF_MAP
 8 accepted prefixes
 8 announced prefixes

Connections established 1; dropped 0
Graceful-restart Status:
 Remote restart-time is 90 sec

 External BGP neighbor may be up to 2 hops away.
Local host: 2001:db8:a::1, Local port: 179
Foreign host: 2001:db8:b::1, Foreign port: 50672
Nexthop: 1.1.1.1
Nexthop global: 2001:db8:a::1
Nexthop local: ::
BGP connection: non shared network
```

If available the following is shown:



- Session information
  - Neighbor address, ASN information and if the link is external or internal
  - BGP version and status
  - Neighbor capabilities for the BGP session
  - Number of messages transmitted and received
- IPv6 unicast address family information
  - BGP4+ table version
  - IPv6 Address Family dependent capabilities
  - IPv6 Communities
  - IPv6 Route filters for ingress and egress updates
  - Number of announced and accepted IPv6 prefixes
- Connection information
  - Connection counters
  - Graceful restart timer
  - Hop count to the peer
  - Next hop information
  - Local and external port numbers

**Related commands** [show ip bgp neighbors \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

## show bgp ipv6 paths (BGP4+ only)

**Overview** Use this command to display BGP4+ path information within an IPv6 environment. Use the [show ip bgp paths \(BGP only\)](#) command to display BGP path information within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 paths`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show bgp ipv6 paths`

**Related commands** [show ip bgp paths \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp ipv6 prefix-list (BGP4+ only)

**Overview** Use this command to display routes matching the prefix-list within an IPv6 environment. Use the [show ip bgp prefix-list \(BGP only\)](#) command to display routes matching the prefix-list within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 prefix-list <list>`

| Parameter | Description                                 |
|-----------|---------------------------------------------|
| <list>    | Specifies the name of the IPv6 prefix list. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show bgp ipv6 prefix-list mylist`

**Related commands** [show ip bgp prefix-list \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp ipv6 quote-regexp (BGP4+ only)

**Overview** Use this command to display routes matching the AS path regular expression within an IPv6 environment. Use the [show ip bgp quote-regexp \(BGP only\)](#) command to display routes matching the AS path regular expression within an IPv4 environment.

Note that you must use quotes to enclose the regular expression with this command. Use the regular expressions listed below with the *<expression>* parameter:

| Symbol | Character     | Meaning                                                                                                                            |
|--------|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| ^      | Caret         | Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match. |
| \$     | Dollar sign   | Used to match the end of the input string.                                                                                         |
| .      | Period        | Used to match a single character (white spaces included).                                                                          |
| *      | Asterisk      | Used to match none or more sequences of a pattern.                                                                                 |
| +      | Plus sign     | Used to match one or more sequences of a pattern.                                                                                  |
| ?      | Question mark | Used to match none or one occurrence of a pattern.                                                                                 |
| _      | Underscore    | Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.                                    |
| [ ]    | Brackets      | Specifies a range of single-characters.                                                                                            |
| -      | Hyphen        | Separates the end points of a range.                                                                                               |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 quote-regexp <expression>`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show bgp ipv6 quote-regexp myexpression`

**Related commands** [show ip bgp quote-regexp \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

## show bgp ipv6 regexp (BGP4+ only)

**Overview** Use this command to display routes matching the AS path regular expression within an IPv6 environment. Use the [show ip bgp regexp \(BGP only\)](#) command to display routes matching the AS path regular expression within an IPv4 environment.

Use the regular expressions listed below with the *<expression>* parameter:

| Symbol | Character     | Meaning                                                                                                                            |
|--------|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| ^      | Caret         | Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match. |
| \$     | Dollar sign   | Used to match the end of the input string.                                                                                         |
| .      | Period        | Used to match a single character (white spaces included).                                                                          |
| *      | Asterisk      | Used to match none or more sequences of a pattern.                                                                                 |
| +      | Plus sign     | Used to match one or more sequences of a pattern.                                                                                  |
| ?      | Question mark | Used to match none or one occurrence of a pattern.                                                                                 |
| _      | Underscore    | Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.                                    |
| [ ]    | Brackets      | Specifies a range of single-characters.                                                                                            |
| -      | Hyphen        | Separates the end points of a range.                                                                                               |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 regexp <expression>`

| Parameter                 | Description                                                 |
|---------------------------|-------------------------------------------------------------|
| <i>&lt;expression&gt;</i> | Specifies a regular-expression to match the BGP4+ AS paths. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show bgp ipv6 regexp myexpression`

**Related commands** [show ip bgp regexp \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series

## Version 5.4.7-2.4: BGP support added for IE300 series

## show bgp ipv6 route-map (BGP4+ only)

**Overview** Use this command to display BGP4+ routes that match the specified route-map within an IPv6 environment. Use the [show ip bgp route-map \(BGP only\)](#) command to display BGP routes that match the specified route-map within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp ipv6 route-map <route-map>`

| Parameter                      | Description                            |
|--------------------------------|----------------------------------------|
| <code>&lt;route-map&gt;</code> | Specifies a route-map that is matched. |

**Mode** User Exec and Privileged Exec

**Example** To show routes that match the route-map `myRouteMap`, use the command:

```
awplus# show bgp ipv6 route-map myRouteMap
```

**Related commands** [show ip bgp route-map \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp ipv6 summary (BGP4+ only)

**Overview** Use this command to display a summary of a BGP4+ neighbor status within an IPv6 environment. Use the [show ip bgp summary \(BGP only\)](#) command to display a summary of a BGP neighbor status within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show bgp ipv6 summary

**Mode** User Exec and Privileged Exec

**Example** awplus# show bgp ipv6 summary

**Output** Figure 24-5: Example output from the **show ip bgp summary** command

```
awplus>show ip bgp summary

BGP router identifier 1.0.0.1, local AS number 65541
BGP table version is 12
4 BGP AS-PATH entries
0 BGP community entries

Neighbor V AS MsgRc MsgSnt TblVer InOutQ Up/Down State/PfxRcd
2001:0db8:cccc::1 4 65544 20 24 11 0/0 00:07:19 1
2001:0db8:dddd::1 4 65545 0 0 0 0/0 never Active
2001:0db8:eeee::1 4 65542 34 40 0 0/0 00:00:04 Active
2001:0db8:ffff::1 4 65543 29 32 11 0/0 00:07:03 13

Number of neighbors 4
```

The Up/Down column in this output is a timer that shows:

- "never" if the peer session has never been established
- The up time, if the peer session is currently up
- The down time, if the peer session is currently down.

In the example above, the session with 2001:0db8:eeee::1 has been down for 4 seconds, and the session with 2001:0db8:dddd::1 has never been established.

**Related commands** [show ip bgp summary \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# show bgp memory maxallocation (BGP only)

**Overview** This command displays the maximum percentage of total memory that is allocated to BGP processes.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show bgp memory maxallocation`

**Mode** User Exec and Privileged Exec

**Example** To display the maximum amount of memory allocated for BGP processes, use the command:

```
awplus# show bgp memory maxallocation
```

**Output** Figure 24-6: Example output from the **show bgp memory maxallocation** command

```
BGP maximum RAM allocation is 100%
```

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp nexthop-tracking (BGP only)

**Overview** Use this command to display BGP next hop tracking status.

**Syntax** `show bgp nexthop-tracking`

**Mode** User Exec and Privileged Exec

**Example** To display BGP next hop tracking status, use the command:

```
awplus# show bgp nexthop-tracking
```

**Related commands** [bgp nexthop-trigger-count](#)  
[show bgp nexthop-tree-details \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show bgp nexthop-tree-details (BGP only)

**Overview** Use this command to display BGP next hop tree details.

**Syntax** `show bgp nexthop-tree-details`

**Mode** User Exec and Privileged Exec

**Example** To display BGP next hop tree details, use the command:

```
awplus# show bgp nexthop-tree-details
```

**Related commands** [show bgp nexthop-tracking \(BGP only\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# show debugging bgp (BGP only)

**Overview** Use this command to see what debugging is turned on for BGP.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show debugging bgp`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show debugging bgp`

**Output** Figure 24-7: Example output from the **show debugging bgp** command

```
BGP debugging status:
 BGP debugging is on
 BGP events debugging is on
 BGP updates debugging is on
 BGP fsm debugging is on
```

**Related commands** [debug bgp \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp (BGP only)

**Overview** Use this command to display BGP network information.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp [<ip-addr>|<ip-addr/m>]`

| Parameter   | Description                                                     |
|-------------|-----------------------------------------------------------------|
| <ip-addr>   | Specifies the IPv4 address and the optional prefix mask length. |
| <ip-addr/m> |                                                                 |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp 10.10.1.34/24`

**Output** Figure 24-8: Example output from the **show ip bgp** command

|                                                                                         |              |        |        |        |   |
|-----------------------------------------------------------------------------------------|--------------|--------|--------|--------|---|
| BGP table version is 7, local router ID is 80.80.80.80                                  |              |        |        |        |   |
| Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S Stale |              |        |        |        |   |
| Origin codes: i - IGP, e - EGP, ? - incomplete                                          |              |        |        |        |   |
| Network                                                                                 | Next Hop     | Metric | LocPrf | Weight |   |
| Path                                                                                    |              |        |        |        |   |
| S>i10.70.0.0/24                                                                         | 192.10.23.67 | 0      | 100    | 0      | ? |
| S>i30.30.30.30/32                                                                       | 192.10.23.67 | 0      | 100    | 0      | ? |
| S>i63.63.63.1/32                                                                        | 192.10.23.67 | 0      | 100    | 0      | ? |
| S>i67.67.67.67/32                                                                       | 192.10.23.67 | 0      | 100    | 0      | ? |
| S>i172.22.10.0/24                                                                       | 192.10.23.67 | 0      | 100    | 0      | ? |
| S>i192.10.21.0                                                                          | 192.10.23.67 | 0      | 100    | 0      | ? |
| S>i192.10.23.0                                                                          | 192.10.23.67 | 0      | 100    | 0      | ? |
| Total number of prefixes 7                                                              |              |        |        |        |   |

**Related commands** [neighbor remove-private-AS \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp attribute-info (BGP only)

**Overview** Use this command to show internal attribute hash information.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp attribute-info`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp attribute-info`

**Output** Figure 24-9: Example output from the **show ip bgp attribute-info** command

```
attr[1] nexthop 0.0.0.0
attr[1] nexthop 10.10.10.10
attr[1] nexthop 10.10.10.50
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp cidr-only (BGP only)

**Overview** Use this command to display routes with non-natural network masks.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp cidr-only`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp cidr-only`

**Output** Figure 24-10: Example output from the **show ip bgp cidr-only** command

```
BGP table version is 0, local router ID is 10.10.10.50

Status codes: s suppressed, d damped, h history, p stale, *
valid, > best, i - internal

Origin codes: i - IGP, e - EGP, ? - incomplete

 Network Next Hop Metric LocPrf Weight Path
*> 3.3.3.0/24 10.10.10.10 0 11 i
*> 6.6.6.0/24 0.0.0.0 32768 i

Total number of prefixes 2
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp community (BGP only)

**Overview** Use this command to display routes that match specified communities from a BGP instance within an IPv4 environment. Use the [show bgp ipv6 community \(BGP4+ only\)](#) command within an IPv6 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

You may use any combination and repetition of parameters listed in the *<type>* placeholder.

**Syntax** `show ip bgp community [<type>] [exact-match]`

| Parameter           | Description                                                                                                 |
|---------------------|-------------------------------------------------------------------------------------------------------------|
| <i>&lt;type&gt;</i> | {[ <i>AA:NN</i> ] [ <i>local-AS</i> ] [ <i>no-advertise</i> ] [ <i>no-export</i> ] }                        |
| <i>AA:NN</i>        | Specifies the Autonomous System (AS) community number, in AA:NN format.                                     |
| <i>local-AS</i>     | Do not send outside local Autonomous Systems (well-known community).                                        |
| <i>no-advertise</i> | Do not advertise to any peer (well-known community).                                                        |
| <i>no-export</i>    | Do not export to next AS (well-known community).                                                            |
| <i>exact-match</i>  | Specifies that the exact match of the communities is displayed. This optional parameter cannot be repeated. |

**Mode** User Exec and Privileged Exec

**Examples** Note that the AS numbers shown are examples only.

```
awplus# show ip bgp community 64497:64499 exact-match
awplus# show ip bgp community 64497:64499 64500:64501
exact-match
awplus# show ip bgp community 64497:64499 64500:64501
64510:64511no-advertise
awplus# show ip bgp community no-advertise
no-advertiseno-advertise exact-match
awplus# show ip bgp community no-export 64510:64511
no-advertise local-AS no-export
awplus# show ip bgp community no-export 64510:64511
no-advertise 64497:64499 64500:64501 no-export
awplus# show ip bgp community no-export 64497:64499
no-advertise local-AS no-export
```



**Related commands**   [set community](#)  
[show bgp ipv6 community \(BGP4+ only\)](#)

**Command changes**   Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp community-info (BGP only)

- Overview** Use this command to list all BGP community information.
- For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).
- Syntax** `show ip bgp community-info`
- Mode** User Exec and Privileged Exec
- Example** `awplus# show ip bgp community-info`
- Command changes**
- Added to AlliedWare Plus prior to 5.4.6-1
  - Version 5.4.7-2.1: BGP support added for x510 and x550 series
  - Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp community-list (BGP only)

**Overview** Use this command to display routes that match the given community-list from a BGP instance within an IPv4 environment. Use the [show bgp ipv6 community-list \(BGP4+ only\)](#) command within an IPv6 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp community-list <listname> [exact-match]`

| Parameter   | Description                                                            |
|-------------|------------------------------------------------------------------------|
| <listname>  | Specifies the community list name.                                     |
| exact-match | Displays only routes that have exactly the same specified communities. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp community-list mylist exact-match`

**Related commands** [show bgp ipv6 community-list \(BGP4+ only\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp dampening (BGP only)

**Overview** Use this command to show dampened routes from a BGP instance within an IPv4 environment. Use the [show bgp ipv6 dampening \(BGP4+ only\)](#) command within an IPv6 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp dampening`  
`{dampened-paths | flap-statistics | parameters}`

| Parameter       | Description                                         |
|-----------------|-----------------------------------------------------|
| dampened-paths  | Display paths suppressed due to dampening.          |
| flap-statistics | Display flap statistics of routes.                  |
| parameters      | Display details of configured dampening parameters. |

**Mode** User Exec and Privileged Exec

**Usage notes** Enable BGP dampening to maintain dampened-path information in memory.

**Examples** `awplus# show ip bgp dampening dampened-paths`

**Output** Figure 24-11: Example output from the **show ip bgp dampening** command

```
dampening 15 750 2000 60 15
Reachability Half-Life time : 15 min
Reuse penalty : 750
Suppress penalty : 2000
Max suppress time : 60 min
Un-reachability Half-Life time : 15 min
Max penalty (ceil) : 11999
Min penalty (floor) : 375
```

The following example output shows that the internal route (i), has flapped 3 times and is now categorized as history (h).

Figure 24-12: Example output from the **show ip bgp dampening flap-statistics** command

```
awplus# show ip bgp dampening flap-statistics
BGP table version is 1, local router ID is 30.30.30.77
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S
Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
 Network From Flaps Duration Reuse Path
 ---- -
hi1.1.1.0/24 10.100.0.62 3 00:01:20 i
```

The following example output shows a dampened route in the 1.1.1.0/24 network.

Figure 24-13: Example output from the **show ip bgp dampening dampened-path** command

```
awplus# show ip bgp dampening dampened-paths
BGP table version is 1, local router ID is 30.30.30.77
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, S
Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

 Network From Reuse Path
di 1.1.1.0/24 10.100.0.62 00:35:10 i

Total number of prefixes 1
```

**Related commands**    [show bgp ipv6 dampening \(BGP4+ only\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp filter-list (BGP only)

**Overview** Use this command to display routes conforming to the filter-list within an IPv4 environment. Use the [show bgp ipv6 filter-list \(BGP4+ only\)](#) command to display routes conforming to the filter-list within an IPv6 environment

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp filter-list <listname>`

| Parameter  | Description                                        |
|------------|----------------------------------------------------|
| <listname> | Specifies the regular-expression access list name. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp filter-list mylist`

**Related commands** [show bgp ipv6 filter-list \(BGP4+ only\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp inconsistent-as (BGP only)

**Overview** Use this command to display routes with inconsistent AS Paths within an IPv4 environment. Use the [show bgp ipv6 inconsistent-as \(BGP4+ only\)](#) command to display routes with inconsistent AS paths within an IPv6 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp inconsistent-as`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp inconsistent-as`

**Related commands** [show bgp ipv6 inconsistent-as \(BGP4+ only\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp longer-prefixes (BGP only)

**Overview** Use this command to display the route of the local BGP routing table for a specific prefix with a specific mask, or for any prefix having a longer mask than the one specified.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp <ip-address/m> longer-prefixes`

| Parameter                         | Description                                                                                              |
|-----------------------------------|----------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-address/m&gt;</code> | Neighbor’s IP address and subnet mask, entered in the form A.B.C.D/M, where M is the subnet mask length. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp 10.10.0.10/24 longer-prefixes`

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series



# show ip bgp neighbors (BGP only)

**Overview** Use this command to display detailed information on peering connections to all BGP neighbors within an IPv4 environment.

Use the [show bgp ipv6 neighbors \(BGP4+ only\)](#) command to display detailed information on peering connections to all BGP4+ neighbors within an IPv6 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax [BGP]** `show ip bgp neighbors [<ipv4-addr> [advertised-routes|received prefix-filter|received-routes|routes]]`

| Parameter              | Description                                                                                                                                     |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv4-addr>            | The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D.                                                                   |
| advertised-routes      | Displays the routes advertised to a BGP neighbor.                                                                                               |
| received prefix-filter | Displays the received prefix-list filters.                                                                                                      |
| received-routes        | Displays the received routes from the neighbor. To display all the received routes from the neighbor, configure the BGP soft reconfigure first. |
| routes                 | Displays all accepted routes learned from neighbors.                                                                                            |

**Mode [BGP]** User Exec and Privileged Exec

**Examples [BGP]**

```
awplus# show ip bgp neighbors 10.10.10.72 advertised-routes
awplus# show ip bgp neighbors 10.10.10.72 received
prefix-filter
awplus# show ip bgp neighbors 10.10.10.72 received-routes
awplus# show ip bgp neighbors 10.10.10.72 routes
```

**Output** Figure 24-14: Example output from **show ip bgp neighbors 10.10.10.72**

```
awplus#show ip bgp neighbors 10.10.10.72
BGP neighbor is 10.10.10.72, remote AS 100, local AS 100, internal
link
Member of peer-group group1 for session parameters
 BGP version 4, remote router ID 0.0.0.0
 BGP state = Active
 Last read , hold time is 90, keepalive interval is 30 seconds
 Received 0 messages, 0 notifications, 0 in queue
 Sent 0 messages, 0 notifications, 0 in queue
 Route refresh request: received 0, sent 0
 Minimum time between advertisement runs is 5 seconds
For address family: IPv4 Unicast
 BGP table version 1, neighbor version 0
 Index 1, Offset 0, Mask 0x2
 group1 peer-group member
 NEXT_HOP is always this router
 0 accepted prefixes
 0 announced prefixes

Connections established 0; dropped 0
Next connect timer due in 33 seconds
```

If available the following is shown:

- Session information
  - Neighbor address, ASN information and if the link is external or internal
  - BGP version and status
  - Neighbor capabilities for the BGP session
  - Number of messages transmitted and received
- IPv4 unicast address family information
  - BGP table version
  - IPv4 Address Family dependent capabilities
  - IPv4 Communities
  - IPv4 Route filters for ingress and egress updates
  - Number of announced and accepted IPv4 prefixes
- Connection information
  - Connection counters
  - Graceful restart timer
  - Hop count to the peer
  - Next hop information
  - Local and external port numbers

**Related commands** [show bgp ipv6 neighbors \(BGP4+ only\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp neighbors connection-retrytime (BGP only)

**Overview** Use this command to display the configured connection-retrytime value of the peer at the session establishment time with the neighbor.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp neighbors <ipv4-addr> connection-retrytime`

| Parameter                      | Description                                                                   |
|--------------------------------|-------------------------------------------------------------------------------|
| <code>&lt;ipv4-addr&gt;</code> | The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp neighbors 10.11.4.26 connection-retrytime`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp neighbors hold-time (BGP only)

**Overview** Use this command to display the configured holdtime value of the peer at the session establishment time with the neighbor.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp neighbors <ipv4-addr> hold-time`

| Parameter                      | Description                                                                   |
|--------------------------------|-------------------------------------------------------------------------------|
| <code>&lt;ipv4-addr&gt;</code> | The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. |

**Default** The holdtime timer default is 90 seconds as per RFC 4271. Holdtime is keepalive \* 3.

**Mode** User Exec and Privileged Exec

**Examples** `awplus# show ip bgp neighbors 10.11.4.26 hold-time`

**Related commands** [neighbor timers](#)  
[show ip bgp neighbors keepalive-interval \(BGP only\)](#)  
[timers \(BGP\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp neighbors keepalive (BGP only)

**Overview** Use this command to display the number of keepalive messages sent to the neighbor from the peer throughout the session.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp neighbors <ipv4-addr> keepalive`

| Parameter                      | Description                                                                   |
|--------------------------------|-------------------------------------------------------------------------------|
| <code>&lt;ipv4-addr&gt;</code> | The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. |

**Mode** User Exec and Privileged Exec

**Examples** `awplus# show ip bgp neighbors 10.11.4.26 keepalive`

**Related commands** [show ip bgp neighbors keepalive-interval \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp neighbors keepalive-interval (BGP only)

**Overview** Use this command to display the configured keepalive-interval value of the peer at the session establishment time with the neighbor.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp neighbors <ipv4-addr> keepalive-interval`

| Parameter   | Description                                                                   |
|-------------|-------------------------------------------------------------------------------|
| <ipv4-addr> | The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. |

**Default** The keepalive timer default is 60 seconds as per RFC 4271. Keepalive is holdtime / 3.

**Mode** User Exec and Privileged Exec

**Examples** `awplus# show ip bgp neighbors 10.11.4.26 keepalive-interval`

**Related commands** [neighbor timers](#)  
[show ip bgp neighbors hold-time \(BGP only\)](#)  
[timers \(BGP\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp neighbors notification (BGP only)

**Overview** Use this command to display the number of notification messages sent to the neighbor from the peer throughout the session.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp neighbors <ipv4-addr> notification`

| Parameter   | Description                                                                   |
|-------------|-------------------------------------------------------------------------------|
| <ipv4-addr> | The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp neighbors 10.11.4.26 notification`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# show ip bgp neighbors open (BGP only)

**Overview** Use this command to display the number of open messages sent to the neighbor from the peer throughout the session.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp neighbors <ipv4-addr> open`

| Parameter                      | Description                                                                   |
|--------------------------------|-------------------------------------------------------------------------------|
| <code>&lt;ipv4-addr&gt;</code> | The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp neighbors 10.11.4.26 open`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp neighbors rcvd-msgs (BGP only)

**Overview** Use this command to display the number of messages received by the neighbor from the peer throughout the session.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp neighbors <ipv4-addr> rcvd-msgs`

| Parameter                      | Description                                                                   |
|--------------------------------|-------------------------------------------------------------------------------|
| <code>&lt;ipv4-addr&gt;</code> | The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp neighbors 10.11.4.26 rcvd-msgs`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp neighbors sent-msgs (BGP only)

**Overview** Use this command to display the number of messages sent to the neighbor from the peer throughout the session.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp neighbors <ipv4-addr> sent-msgs`

| Parameter                      | Description                                                                   |
|--------------------------------|-------------------------------------------------------------------------------|
| <code>&lt;ipv4-addr&gt;</code> | The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp neighbors 10.11.4.26 sent-msgs`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp neighbors update (BGP only)

**Overview** Use this command to display the number of update messages sent to the neighbor from the peer throughout the session.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp neighbors <ipv4-addr> update`

| Parameter                      | Description                                                                   |
|--------------------------------|-------------------------------------------------------------------------------|
| <code>&lt;ipv4-addr&gt;</code> | The IPv4 address of an IPv4 BGP neighbor, in dotted decimal notation A.B.C.D. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp neighbors 10.11.4.26 update`

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp paths (BGP only)

**Overview** Use this command to display BGP4 path information within an IPv4 environment. Use the [show bgp ipv6 paths \(BGP4+ only\)](#) command to display BGP4+ path information within an IPv4 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp paths`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp paths`

**Related commands** [show bgp ipv6 paths \(BGP4+ only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp prefix-list (BGP only)

**Overview** Use this command to display routes matching the prefix-list within an IPv4 environment. Use the [show bgp ipv6 prefix-list \(BGP4+ only\)](#) command to display routes matching the prefix-list within an IPv6 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp prefix-list <list>`

| Parameter | Description                               |
|-----------|-------------------------------------------|
| <list>    | Specifies the name of the IP prefix list. |

**Mode** User Exec and Privileged Exec

**Examples** `awplus# show ip bgp prefix-list mylist`

**Related commands** [show bgp ipv6 prefix-list \(BGP4+ only\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp quote-regexp (BGP only)

**Overview** Use this command to display routes matching the AS path regular expression within an IPv4 environment. Use the [show bgp ipv6 quote-regexp \(BGP4+ only\)](#) command to display routes matching the AS path regular expression within an IPv6 environment.

Note that you must use quotes to enclose the regular expression with this command. Use the regular expressions listed below with the *<expression>* parameter:

| Symbol | Character     | Meaning                                                                                                                            |
|--------|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| ^      | Caret         | Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match. |
| \$     | Dollar sign   | Used to match the end of the input string.                                                                                         |
| .      | Period        | Used to match a single character (white spaces included).                                                                          |
| *      | Asterisk      | Used to match none or more sequences of a pattern.                                                                                 |
| +      | Plus sign     | Used to match one or more sequences of a pattern.                                                                                  |
| ?      | Question mark | Used to match none or one occurrence of a pattern.                                                                                 |
| _      | Underscore    | Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.                                    |
| [ ]    | Brackets      | Specifies a range of single-characters.                                                                                            |
| -      | Hyphen        | Separates the end points of a range.                                                                                               |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp quote-regexp <expression>`

| Parameter                 | Description                                               |
|---------------------------|-----------------------------------------------------------|
| <i>&lt;expression&gt;</i> | Specifies a regular-expression to match the BGP AS paths. |

**Mode** User Exec and Privileged Exec

**Examples** `awplus# show ip bgp quote-regexp myexpression`

**Related commands** [show bgp ipv6 quote-regexp \(BGP4+ only\)](#)

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series



## show ip bgp regexp (BGP only)

**Overview** Use this command to display routes matching the AS path regular expression within an IPv4 environment. Use the [show bgp ipv6 regexp \(BGP4+ only\)](#) command to display routes matching the AS path regular expression within an IPv6 environment.

Use the regular expressions listed below with the *<expression>* parameter:

| Symbol | Character     | Meaning                                                                                                                            |
|--------|---------------|------------------------------------------------------------------------------------------------------------------------------------|
| ^      | Caret         | Used to match the beginning of the input string. When used at the beginning of a string of characters, it negates a pattern match. |
| \$     | Dollar sign   | Used to match the end of the input string.                                                                                         |
| .      | Period        | Used to match a single character (white spaces included).                                                                          |
| *      | Asterisk      | Used to match none or more sequences of a pattern.                                                                                 |
| +      | Plus sign     | Used to match one or more sequences of a pattern.                                                                                  |
| ?      | Question mark | Used to match none or one occurrence of a pattern.                                                                                 |
| _      | Underscore    | Used to match spaces, commas, braces, parenthesis, or the beginning and end of an input string.                                    |
| [ ]    | Brackets      | Specifies a range of single-characters.                                                                                            |
| -      | Hyphen        | Separates the end points of a range.                                                                                               |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp regexp <expression>`

| Parameter                 | Description                                               |
|---------------------------|-----------------------------------------------------------|
| <i>&lt;expression&gt;</i> | Specifies a regular-expression to match the BGP AS paths. |

**Mode** User Exec and Privileged Exec

**Examples** `awplus# show ip bgp regexp myexpression`

**Related commands** [show bgp ipv6 regexp \(BGP4+ only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp route-map (BGP only)

**Overview** Use this command to display BGP routes that match the specified route-map within an IPv4 environment. Use the [show bgp ipv6 route-map \(BGP4+ only\)](#) command to display BGP4+ routes that match the specified route-map within an IPv6 environment.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp route-map <route-map>`

| Parameter                      | Description                            |
|--------------------------------|----------------------------------------|
| <code>&lt;route-map&gt;</code> | Specifies a route-map that is matched. |

**Mode** User Exec and Privileged Exec

**Examples** To show routes that match the route-map `myRouteMap`, use the command:

```
awplus# show ip bgp route-map myRouteMap
```

**Related commands** [show bgp ipv6 route-map \(BGP4+ only\)](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

## show ip bgp scan (BGP only)

**Overview** Use this command to display BGP scan status.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip bgp scan`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip bgp scan`

**Output** Figure 24-15: Example output from the **show ip bgp scan** command

```
BGP scan is running
BGP scan interval is 60
BGP instance : AS is 11,DEFAULT
Current BGP nexthop cache:
BGP connected route:
 10.10.10.0/24
 10.10.11.0/24
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# show ip bgp summary (BGP only)

**Overview** Use this command to display a summary of a BGP neighbor status within an IPv4 environment. Use the [show bgp ipv6 summary \(BGP4+ only\)](#) command to display a summary of BGP4+ neighbors.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show ip bgp summary

**Mode** User Exec and Privileged Exec

**Examples** awplus# show ip bgp summary

**Output** Figure 24-16: Example output from the **show ip bgp summary** command

```
awplus>show ip bgp summary

BGP router identifier 1.0.0.1, local AS number 65541
BGP table version is 12
4 BGP AS-PATH entries
0 BGP community entries

Neighbor V AS MsgRc MsgSnt TblVer InOutQ Up/Down State/PfxRcd
192.168.3.2 4 65544 20 24 11 0/0 00:07:19 1
192.168.4.2 4 65545 0 0 0 0/0 never Active
192.168.11.2 4 65542 34 40 0 0/0 00:00:04 Active
192.168.21.2 4 65543 29 32 11 0/0 00:07:03 13

Number of neighbors 4
```

The Up/Down column in this output is a timer that shows:

- "never" if the peer session has never been established
- The up time, if the peer session is currently up
- The down time, if the peer session is currently down.

In the example above, the session with 192.168.11.2 has been down for 4 seconds, and the session with 192.168.4.2 has never been established.

**Related commands** [show bgp ipv6 summary \(BGP4+ only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.6-2.1: VRF-lite support added to BGP for AR-series products  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip community-list

**Overview** Use this command to display routes that match a specified community-list name or number.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip community-list [<listnumber>|<listname>]`

| Parameter    | Description                                                                                                                    |
|--------------|--------------------------------------------------------------------------------------------------------------------------------|
| <listnumber> | Specifies the community list number in the range <1-199> as specified by a previously issued <b>ip community-list</b> command. |
| <listname>   | Specifies the community list name as specified by a previously issued <a href="#">ip community-list</a> command.               |

**Mode** User Exec and Privileged Exec

**Examples** `awplus# show ip community-list mylist`  
`awplus# show ip community-list 99`

**Related commands** [ip community-list](#)  
[ip community-list expanded](#)  
[ip community-list standard](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip extcommunity-list

**Overview** Use this command to display a configured extcommunity-list.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip extcommunity-list [<1-199>|<extcommunity-listname>]`

| Parameter               | Description              |
|-------------------------|--------------------------|
| <1-199>                 | Extcommunity-list number |
| <extcommunity-listname> | Extcommunity-list name   |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip extcommunity-list 33`

**Related commands** [ip extcommunity-list expanded](#)  
[ip extcommunity-list standard](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show ip prefix-list

**Overview** Use this command to display the IPv4 prefix-list entries.  
Note that this command is valid for RIP and BGP routing protocols only.

**Syntax** `show ip prefix-list [<name>|detail|summary]`

| Parameter | Description                                                               |
|-----------|---------------------------------------------------------------------------|
| <name>    | Specify the name of a prefix list in this placeholder.                    |
| detail    | Specify this parameter to show detailed output for all IPv4 prefix lists. |
| summary   | Specify this parameter to show summary output for all IPv4 prefix lists.  |

**Mode** User Exec and Privileged Exec

**Example**

```
awplus# show ip prefix-list
awplus# show ip prefix-list 10.10.0.98/8
awplus# show ip prefix-list detail
```

**Related commands** [ip prefix-list](#)



# show ipv6 prefix-list

**Overview** Use this command to display the prefix-list entries.

Note that this command is valid for RIPv6 and BGP4+ routing protocols only.

**Syntax** `show ipv6 prefix-list [<name>|detail|summary]`

| Parameter | Description                                                               |
|-----------|---------------------------------------------------------------------------|
| <name>    | Specify the name of an individual IPv6 prefix list.                       |
| detail    | Specify this parameter to show detailed output for all IPv6 prefix lists. |
| summary   | Specify this parameter to show summary output for all IPv6 prefix lists.  |

**Mode** User Exec and Privileged Exec

**Example**

```
awplus# show ipv6 prefix-list
awplus# show ipv6 prefix-list 10.10.0.98/8
awplus# show ipv6 prefix-list detail
```

**Related commands** [ipv6 prefix-list](#)

# show ip protocols bgp (BGP only)

**Overview** Use this command to display BGP process parameters and statistics.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip protocols bgp`

**Mode** User Exec and Privileged Exec

**Example** To display BGP process parameters and statistics, use the command:

```
awplus# show ip protocols bgp
```

**Output** Figure 24-17: Example output from the **show ip protocols bgp** command

```
Routing Protocol is "bgp 100"
 IGP synchronization is disabled
 Automatic route summarization is disabled
 Default local-preference applied to incoming route is 100
 Redistributing:
 Neighbor(s):
 Address AddressFamily FiltIn FiltOut DistIn DistOut RouteMapIn RouteMapOut
Weight
10.10.10.1 unicast
```

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# show route-map

**Overview** Use this command to display information about one or all route maps.

**Syntax** `show route-map <map-name>`

| Parameter                     | Description                       |
|-------------------------------|-----------------------------------|
| <code>&lt;map-name&gt;</code> | A name to identify the route map. |

**Mode** User Exec and Privileged Exec

**Example** To display information about the route-map named `example-map`, use the command:

```
awplus# show route-map example-map
```

**Output** Figure 24-18: Example output from the **show route-map** command

```
route-map example-map, permit, sequence 1
 Match clauses:
 ip address prefix-list example-pref
 Set clauses:
 metric 100
route-map example-map, permit, sequence 200
 Match clauses:
 Set clauses:
```

**Related commands** [route-map](#)

# synchronization

**Overview** Use this command in Router Configuration mode or in Address Family Configuration mode to ensure BGP does not advertise router learned from iBGP peers until they are learned locally, or are propagated throughout the AS via an IGP.

Use the **no** variant of this command to disable this function.

**Syntax** `synchronization`  
`no synchronization`

**Default** Disabled.

**Mode** Router Configuration and Address Family Configuration mode

**Usage notes** Synchronization is used when a BGP router should not advertise routes learned from iBGP neighbors, unless those routes are also present in an IGP (for example, OSPF). These routes must be in the RIB (Routing Information Base) learned locally or via an IGP.

Synchronization may be enabled when all the routers in an autonomous system do not speak BGP, and the autonomous system is a transit for other autonomous systems.

Use the **no synchronization** command when BGP router can advertise routes learned from iBGP neighbors, without waiting for IGP reachability, when routes are in the RIB.

**Example** The following example enables IGP synchronization of iBGP routes in Router Configuration mode:

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config-router)# synchronization
```

The following example enables IGP synchronization of iBGP routes in IPv4 unicast Address Family Configuration mode:

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config)# address-family ipv4 unicast
awplus(config-af)# synchronization
```

The following example enables IGP synchronization of iBGP routes in the IPv6 unicast Address Family Configuration mode:

```
awplus# configure terminal
awplus(config)# router bgp 11
awplus(config)# address-family ipv6 unicast
awplus(config-af)# synchronization
```

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# timers (BGP)

**Overview** Use this command sets the BGP keepalive timer and holdtime timer values.  
Use the **no** variant of this command to reset timers to the default.

**Syntax** `timers bgp <keepalive> <holdtime>`  
`no timers bgp [<keepalive> <holdtime>]`

| Parameter   | Description                                                                                                                                                                                                                                                                                                                                     |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <keepalive> | <0-65535> The frequency with which the keepalive messages are sent to the neighbors. The default is 30 seconds as per RFC 4271. Cisco IOS uses a 60 second keepalive timer default value. Adjust keepalive timers for interoperability as required. Maintain the keepalive value at the holdtime value / 3.                                     |
| <holdtime>  | <0-65535> The interval after which the neighbor is considered dead if keepalive messages are not received. The default holdtime value is 90 seconds as per RFC 4271. Cisco IOS uses a 180 second holdtime timer default value. Adjust holdtime timers for interoperability as required. Maintain the holdtime value at the keepalive value * 3. |

**Default** The keepalive timer default is 60 seconds, the holdtime timer default is 90 seconds, and the connect timer default is 120 seconds as per RFC 4271. Holdtime is keepalive \* 3.

**Mode** Router Configuration

**Usage notes** This command is used globally to set or unset the keepalive and holdtime values for all the neighbors.

**Examples**

```
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# timers bgp 40 120
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no timers bgp 30 90
awplus# configure terminal
awplus(config)# router bgp 10
awplus(config-router)# no timers bgp
```

**Related commands** [neighbor timers](#)  
[show ip bgp neighbors hold-time \(BGP only\)](#)  
[show ip bgp neighbors keepalive-interval \(BGP only\)](#)

**Command  
changes**

Added to AlliedWare Plus prior to 5.4.6-1

Version 5.4.7-2.1: BGP support added for x510 and x550 series

Version 5.4.7-2.4: BGP support added for IE300 series

# undebg bgp (BGP only)

**Overview** Use this command to disable BGP debugging functions.

**Syntax** undebg bgp  
[all|dampening|events|filters|fsm|keepalives|nht|nsm|updates]  
undebg all bgp

| Parameter  | Description                                                 |
|------------|-------------------------------------------------------------|
| all        | Disable all debugging for BGP.                              |
| dampening  | Disable debugging for BGP dampening.                        |
| events     | Disable debugging for BGP events.                           |
| filters    | Disable debugging for BGP filters.                          |
| fsm        | Disable debugging for BGP Finite State Machine (FSM).       |
| keepalives | Disable debugging for BGP keepalives.                       |
| nht        | Disable debugging for BGP NHT (Next Hop Tracking) messages. |
| nsm        | Disable debugging for NSM messages.                         |
| updates    | Disable debugging for BGP updates.                          |

**Mode** Privileged Exec and Global Configuration

**Example** awplus# undebg bgp events  
awplus# undebg bgp nht  
awplus# undebg bgp updates

**Related commands** [debug bgp \(BGP only\)](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series



# 25

# Route Map Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for route map commands. For more information, see the [Routemaps Feature Overview and Configuration Guide](#). These commands can be divided into the following categories:

- the [route-map](#) command, which is used to create a route map and/or route map entry, and to put you into route map mode
- **match** commands, used to determine which routes or BGP update messages the route map applies to
- **set** commands, used to modify matching routes or BGP update messages

- Command List**
- ["match as-path"](#) on page 1215
  - ["match community"](#) on page 1216
  - ["match interface"](#) on page 1218
  - ["match ip address"](#) on page 1219
  - ["match ip next-hop"](#) on page 1221
  - ["match ipv6 address"](#) on page 1223
  - ["match ipv6 next-hop"](#) on page 1225
  - ["match metric"](#) on page 1226
  - ["match origin"](#) on page 1227
  - ["match route-type"](#) on page 1229
  - ["match tag"](#) on page 1230
  - ["route-map"](#) on page 1231
  - ["set aggregator"](#) on page 1234
  - ["set as-path"](#) on page 1235
  - ["set atomic-aggregate"](#) on page 1236

- [“set comm-list delete”](#) on page 1237
- [“set community”](#) on page 1238
- [“set dampening”](#) on page 1240
- [“set extcommunity”](#) on page 1242
- [“set ip next-hop \(route map\)”](#) on page 1244
- [“set ipv6 next-hop”](#) on page 1245
- [“set local-preference”](#) on page 1246
- [“set metric”](#) on page 1247
- [“set metric-type”](#) on page 1249
- [“set origin”](#) on page 1250
- [“set originator-id”](#) on page 1251
- [“set tag”](#) on page 1252
- [“set weight”](#) on page 1253
- [“show route-map”](#) on page 1254

# match as-path

**Overview** Use this command to add an autonomous system (AS) path match clause to a route map entry. Specify the AS path attribute value or values to match by specifying the name of an AS path access list.

A BGP update message matches the route map if its attributes include AS path values that match the AS path access list.

Each entry of a route map can only match against one AS path access list in one AS path match clause. If the route map entry already has an AS path match clause, entering this command replaces that match clause with the new clause.

Note that AS path access lists and route map entries both specify an action of deny or permit. The action in the AS path access list determines whether the route map checks update messages for a given AS path value. The route map action and its **set** clauses determine what the route map does with update messages that contain that AS path value.

Use the **no** variant of this command to remove the AS path match clause from a route map entry.

**Syntax** `match as-path <as-path-listname>`  
`no match as-path [<as-path-listname>]`

| Parameter                             | Description                            |
|---------------------------------------|----------------------------------------|
| <code>&lt;as-path-listname&gt;</code> | Specifies an AS path access list name. |

**Mode** Route-map Configuration

**Usage notes** This command is valid for BGP update messages only.

**Example** To add entry 34 to the route map called `myroute`, which will discard update messages if they contain the AS path values that are included in `myaccesslist`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute deny 34
awplus(config-route-map)# match as-path myaccesslist
```

**Related commands** [route-map](#)  
[set as-path](#)  
[show route-map](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# match community

**Overview** Use this command to add a community match clause to a route map entry. Specify the community value or values to match by specifying a community list. To create the community list, enter Global Configuration mode and use the [ip community-list](#) command.

A BGP update message matches the route map if its attributes include community values that match the community list.

Each entry of a route map can only match against one community list in one community match clause. If the route map entry already has a community match clause, entering this command replaces that match clause with the new clause.

Note that community lists and route map entries both specify an action of deny or permit. The action in the community list determines whether the route map checks update messages for a given community value. The route map action and its **set** clauses determine what the route map does with update messages that contain that community value.

Use the **no** variant of this command to remove the community match clause from a route map.

**Syntax**

```
match community
{<community-listname>|<1-99>|<100-199>} [exact-match]

no match community
[<community-listname>|<1-99>|<100-199>|exact-match]
```

| Parameter            | Description                             |
|----------------------|-----------------------------------------|
| <community-listname> | The community list name or number.      |
| <1-99>               | Community list number (standard range). |
| <100-199>            | Community list number (expanded range). |
| exact-match          | Exact matching of communities.          |

**Mode** Route-map Configuration

**Usage notes** This command is valid for BGP update messages only.

Communities are used to group and filter routes. They are designed to provide the ability to apply policies to large numbers of routes by using match and set commands. Community lists are used to identify and filter routes by their common attributes.

**Example** To add entry 3 to the route map called `myroute`, which will process update messages if they contain the community values that are included in `mylist`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# match community mylist
```

**Related commands**

- `ip community-list`
- `route-map`
- `set comm-list delete`
- `set community`
- `show route-map`

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# match interface

**Overview** Use this command to add an interface match clause to a route map entry. Specify the interface name to match.

A route matches the route map if its interface matches the interface name.

Each entry of a route map can only match against one interface in one interface match clause. If the route map entry already has an interface match clause, entering this command replaces that match clause with the new clause.

Use the **no** variant of this command to remove the interface match clause from the route map entry. Use the **no** variant of this command without a specified interface to remove all interfaces.

**Syntax** `match interface <interface>`  
`no match interface [<interface>]`

| Parameter                      | Description             |
|--------------------------------|-------------------------|
| <code>&lt;interface&gt;</code> | The interface to match. |

**Mode** Route-map Configuration

**Usage** This command is valid for RIP and OSPF routes only.

**Example** To add entry 10 to the route map called 'mymap1', which will process routes if they use the interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# route-map mymap1 permit 10
awplus(config-route-map)# match interface eth1
```

To remove all interfaces from the route map called 'mymap1', use the commands:

```
awplus# configure terminal
awplus(config)# route-map mymap1 permit 10
awplus(config-route-map)# no match interface
```

**Related commands**

- [match ip address](#)
- [match ip next-hop](#)
- [match route-type](#)
- [match tag](#)
- [route-map](#)
- [show route-map](#)

# match ip address

**Overview** Use this command to add an IP address prefix match clause to a route map entry. You can specify the prefix or prefixes to match by specifying the name of the prefix list. To create the prefix list, enter Global Configuration mode and use the **ip prefix-list** command.

A route matches the route map entry if the route's prefix matches the prefix list.

Use the **no** variant of this command to remove the IP address match clause from a route map entry.

**Syntax** `match ip address prefix-list <prefix-listname>`  
`no match ip address prefix-list <prefix-listname>`

| Parameter   | Description                                               |
|-------------|-----------------------------------------------------------|
| prefix-list | Use an IP prefix list to specify which prefixes to match. |
|             | <prefix-listname> The prefix list name.                   |

**Mode** Route-map Configuration

**Usage notes** Each entry of a route map can have at most one prefix list-based IP address match clause. If the route map entry already has one match clause, entering this command replaces that match clause with the new clause.

Note that prefix lists and route map entries both specify an action of deny or permit. The action in the prefix list determines whether the route map checks update messages and routes for a given prefix. The action in the route map, and the map's **set** clauses, determine what the device does with update messages or routes that contain that prefix.

If the **match ip address** command results in a match against the specified IP address, then the outcome is:

- If **permit** is specified, then the route is redistributed or controlled, as specified by the set action.
- If **deny** is specified, then the route is not redistributed or controlled.

If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of **permit** or **deny** specifications.

This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

**Examples** To add entry 3 to the route map called 'rmap1', which will process routes that match the prefix list called 'mylist', use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# match ip address prefix-list mylist
```

**Related commands** [route-map](#)  
[show route-map](#)



# match ip next-hop

**Overview** Use this command to add a next-hop match clause to a route map entry. You can specify the next hop to match by specifying the name of a prefix list. To create the prefix list, enter Global Configuration mode and use the **ip prefix-list** command.

A route matches the route map if the route's next hop matches the prefix list.

Each entry of a route map can have at most one prefix list-based next-hop match clause. If the route map entry already has one match clause, entering this command replaces that match clause with the new clause.

Note that the lists and route map entries specify an action of deny or permit. The action in the list determines whether the route map checks update messages and routes for a given next-hop value. The route map action and its **set** clauses determine what the route map does with update messages and routes that contain that next hop.

Use the **no** variant of this command to remove the next-hop match clause from a route map entry. To remove a prefix list-based match clause you must also specify the prefix-list parameter.

**Syntax** `match ip next-hop prefix-list <prefix-listname>`  
`no match ip next-hop prefix-list [<prefix-listname>]`

| Parameter   | Description                                                |
|-------------|------------------------------------------------------------|
| prefix-list | Use an IP prefix list to specify which next hops to match. |
|             | <code>&lt;prefix-listname&gt;</code> The prefix list name. |

**Mode** Route-map Configuration

**Usage notes** This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

**Examples** To add entry 3 to the route map called 'mymap', which will process routes whose next hop matches the prefix list called 'list1', use the commands:

```
awplus# configure terminal
awplus(config)# route-map mymap permit 3
awplus(config-route-map)# match ip next-hop prefix-list list1
```

**Related  
commands**

- ip prefix-list
- route-map
- show ip prefix-list
- show route-map

# match ipv6 address

**Overview** Use this command to add an IPv6 address prefix match clause to a route map entry. You can specify the prefix or prefixes to match by specifying the name of the prefix list. To create the prefix list, enter Global Configuration mode and use the **ipv6 prefix-list** command.

A route matches the route map entry if the route's prefix matches the prefix list.

Use the **no** variant of this command to remove the IPv6 address match clause from a route map entry.

**Syntax**

```
match ipv6 address prefix-list <prefix-listname>
no match ipv6 address
no match ipv6 address prefix-list <prefix-listname>
```

| Parameter         | Description                                               |
|-------------------|-----------------------------------------------------------|
| prefix-list       | Use an IP prefix list to specify which prefixes to match. |
| <prefix-listname> | The prefix list name.                                     |

**Mode** Route-map Configuration

**Usage notes** Each entry of a route map can have at most one prefix list-based IPv6 address match clause. If the route map entry already has one match clause, entering this command replaces that match clause with the new clause.

Note that prefix lists and route map entries all specify an action of deny or permit. The action in the prefix list determines whether the route map checks update messages and routes for a given prefix. The action in the route map, and the map's **set** clauses, determine what the device does with update messages or routes that contain that prefix.

If the **match ipv6 address** command results in a match against the specified IPv6 address, then the outcome is:

- If **permit** is specified, then the route is redistributed or controlled, as specified by the set action.
- If **deny** is specified, then the route is not redistributed or controlled.

If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of **permit** or **deny** specifications.

This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

**Examples** To match traffic according to the prefix list named "mylist", use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# match ipv6 address prefix-list mylist
```

# match ipv6 next-hop

**Overview** Use this command to specify a next-hop address to be matched by the route-map. Use the **no** variant of this command to disable this function.

**Syntax**

```
match ipv6 next-hop <ipv6-addr>
match ipv6 next-hop prefix-list <prefix-listname>
match ipv6 next-hop [<ipv6-addr>]
match ipv6 next-hop [prefix-list <prefix-listname>]
```

| Parameter         | Description                                                                               |
|-------------------|-------------------------------------------------------------------------------------------|
| <ipv6-addr>       | The IPv6 address of the next hop. The IPv6 address uses the format X:X::X:X.              |
| <prefix-listname> | The name of the IPv6 prefix list that specifies criteria for the addresses to be matched. |

**Mode** Route-map Configuration

**Usage notes** The **match ipv6 next-hop** command specifies the next-hop address to be matched. If there is a match for the specified next-hop address, and permit is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and deny is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of permit or deny specifications.

**NOTE:** This command is valid only for BGP.

**Example**

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# match ipv6 next-hop 2001:0db8::/32
```

# match metric

**Overview** Use this command to add a metric match clause to a route map entry. Specify the metric value to match.

A route matches the route map if its metric matches the route map's metric.

A BGP update message matches the route map if its MED attribute value matches the route map's metric.

Each entry of a route map can only match against one metric value in one metric match clause. If the route map entry already has a metric match clause, entering this command replaces that match clause with the new clause.

Use the **no** variant of this command to remove the metric match clause from the route map entry.

**Syntax** `match metric <metric>`  
`no match metric [<metric>]`

| Parameter | Description                                |
|-----------|--------------------------------------------|
| <metric>  | <0-4294967295> Specifies the metric value. |

**Mode** Route-map Configuration

**Usage notes** This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

**Example** To stop entry 3 of the route map called "myroute" from processing routes with a metric of 888999, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# no match metric 888999
```

**Related commands** [route-map](#)  
[set metric](#)  
[show route-map](#)

# match origin

**Overview** Use this command to add an origin match clause to a route map entry. Specify the origin attribute value to match.

A BGP update message matches the route map if its origin attribute value matches the route map's origin value.

Each entry of a route map can only match against one origin in one origin match clause. If the route map entry already has an origin match clause, entering this command replaces that match clause with the new clause.

Use the **no** variant of this command to remove the origin match clause from the route map entry.

**Syntax** `match origin {egp|igp|incomplete}`  
`no match origin [egp|igp|incomplete]`

| Parameter  | Description                                      |
|------------|--------------------------------------------------|
| egp        | Learned from an exterior gateway protocol.       |
| igp        | Learned from a local interior gateway protocol.  |
| incomplete | Of unknown heritage, for example a static route. |

**Mode** Route-map Configuration

**Usage** The origin attribute defines the origin of the path information. The **egp** parameter is indicated as an **e** in the routing table, and it indicates that the origin of the information is learned via Exterior Gateway Protocol. The **igp** parameter is indicated as an **i** in the routing table, and it indicates the origin of the path information is interior to the originating AS. The **incomplete** parameter is indicated as a **?** in the routing table, and indicates that the origin of the path information is unknown or learned through other means. If a static route is redistributed into BGP, the origin of the route is incomplete.

The **match origin** command specifies the origin to be matched. If there is a match for the specified origin, and **permit** is specified, the route is redistributed or controlled as specified by the set action. If the match criteria are met, and **deny** is specified, the route is not redistributed or controlled. If the match criteria are not met, the route is neither accepted nor forwarded, irrespective of **permit** or **deny** specifications.

This command is valid for BGP update messages only.

**Example** To add entry 34 to the route map called "rmap1", which will drop externally-originated routes, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute deny 34
awplus(config-route-map)# match origin egp
```

**Related  
commands**   route-map  
                  set origin  
                  show route-map



# match route-type

**Overview** Use this command to add an external route-type match clause to a route map entry. Specify whether to match OSPF type-1 external routes or OSPF type-2 external routes.

An OSPF route matches the route map if its route type matches the route map's route type.

Each entry of a route map can only match against one route type in one match clause. If the route map entry already has a route type match clause, entering this command replaces that match clause with the new clause.

Use the **no** variant of this command to remove the route type match clause from the route map entry.

**Syntax** `match route-type external {type-1|type-2}`  
`no match route-type external [type-1|type-2]`

| Parameter | Description                  |
|-----------|------------------------------|
| type-1    | OSPF type-1 external routes. |
| type-2    | OSPF type-2 external routes. |

**Mode** Route-map Configuration

**Usage** Use the **match route-type external** command to match specific external route types. AS- external LSA is either Type-1 or Type-2. **external type-1** matches only Type 1 external routes, and **external type-2** matches only Type 2 external routes. This command is valid for OSPF routes only.

**Example** To add entry 10 to the route map called `mymap1`, which will process type-1 external routes, use the commands:

```
awplus# configure terminal
awplus(config)# route-map mymap1 permit 10
awplus(config-route-map)# match route-type external type-1
```

**Related commands**

- [match interface](#)
- [match ip address](#)
- [match ip next-hop](#)
- [match tag](#)
- [route-map](#)
- [set metric-type](#)
- [show route-map](#)

# match tag

**Overview** Use this command to add a tag match clause to a route map entry. Specify the route tag value to match.

An OSPF route matches the route map if it has been tagged with the route map's tag value. Routes can be tagged through OSPF commands or through another route map's set clause.

Each entry of a route map can only match against one tag in one match clause. If the route map entry already has a tag match clause, entering this command replaces that match clause with the new clause.

Use the **no** variant of this command to remove the tag match clause from the route map entry.

**Syntax** `match tag <0-4294967295>`  
`no match tag [<0-4294967295>]`

**Mode** Route-map Configuration

**Usage** This command is valid for OSPF routes only.

**Example** To add entry 10 to the route map called `mymap1`, which will process routes that are tagged 100, use the following commands:

```
awplus# configure terminal
awplus(config)# route-map mymap1 permit 10
awplus(config-route-map)# match tag 100
```

**Related commands**

- [match interface](#)
- [match ip address](#)
- [match ip next-hop](#)
- [match route-type](#)
- [route-map](#)
- [set tag](#)
- [show route-map](#)

# route-map

**Overview** Use this command to configure a route map entry, and to specify whether the device will process or discard matching routes and BGP update messages.

The device uses a name to identify the route map, and a sequence number to identify each entry in the route map.

The **route-map** command puts you into route-map configuration mode. In this mode, you can use the following:

- one or more of the **match** commands to create match clauses. These specify what routes or update messages match the entry.
- one or more of the **set** commands to create set clauses. These change the attributes of matching routes or update messages.

Use the **no** variant of this command to delete a route map or to delete an entry from a route map.

**Syntax**

```
route-map <mapname> {deny|permit} <seq>
no route-map <mapname>
no route-map <mapname> {deny|permit} <seq>
```

| Parameter | Description                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------|
| <mapname> | A name to identify the route map.                                                                                         |
| deny      | The route map causes a routing process to discard matching routes or BGP update messages.                                 |
| permit    | The route map causes a routing process to use matching routes or BGP update messages.                                     |
| <seq>     | <1-65535> The sequence number of the entry. You can use this parameter to control the order of entries in this route map. |

**Mode** Global Configuration

**Usage notes** Route maps allow you to control and modify routing information by filtering routes and setting route attributes. You can apply route maps when the device:

- processes BGP update messages that it has received from a peer
- prepares BGP update messages to send to peers
- redistributes routes from one routing protocol into another
- redistributes static routes into routing protocols
- uses BGP route flap dampening

When a routing protocol passes a route or update message through a route map, it checks the entries in order of their sequence numbers, starting with the lowest numbered entry.

If it finds a match on a route map with an action of permit, then it applies any set clauses and accepts the route. Having found a match, the route is not compared against any further entries of the route map.

If it finds a match on a route map with an action of deny, it will discard the matching route.

If it does not find a match, it discards the route or update message. This means that route maps end with an implicit deny entry. To permit all non-matching routes or update messages, end your route map with an entry that has an action of **permit** and no match clause.

**Examples** To enter route-map mode for entry 1 of the route map called "route1", and then add a match and set clause to it, use the commands:

```
awplus# configure terminal
awplus(config)# route-map route1 permit 1
awplus(config-route-map)# match as-path 60
awplus(config-route-map)# set weight 70
```

To enter route-map mode for entry 2 of the route map called "route1", and then add a match and set clause to it, use the commands:

```
awplus# configure terminal
awplus(config)# route-map route1 permit 2
awplus(config-route-map)# match interface eth1
awplus(config-route-map)# set metric 20
```

Note how the prompt changes when you go into route map configuration mode.

To make the device process non-matching routes instead of discarding them, add a command like the following one:

```
awplus(config)# route-map route1 permit 100
```

**Related  
commands**

For BGP:

- [show route-map](#)
- [bgp dampening](#)
- [neighbor default-originate](#)
- [neighbor route-map](#)
- [neighbor unsuppress-map](#)
- [network \(BGP and BGP4+\)](#)
- [redistribute \(into BGP or BGP4+\)](#)
- [show ip bgp route-map \(BGP only\)](#)

For OSPF:

- [default-information originate](#)
- [redistribute \(OSPF\)](#)

For RIP:

`redistribute (RIP)`

# set aggregator

**Overview** Use this command to add an aggregator set clause to a route map entry.

When a BGP update message matches the route map entry, the device sets the update's aggregator attribute. The aggregator attribute specifies the AS and IP address of the device that performed the aggregation.

Use the **no** variant of this command to remove the set clause.

**Syntax** `set aggregator as <asnum> <ip-address>`  
`no set aggregator as`

| Parameter    | Description                       |
|--------------|-----------------------------------|
| <asnum>      | The AS number of the aggregator.  |
| <ip-address> | The IP address of the aggregator. |

**Mode** Route-map Configuration

**Usage** An Autonomous System (AS) is a collection of networks under a common administration sharing a common routing strategy. It is subdivided by areas, and is assigned a unique 16-bit number. Use the **set aggregator** command to assign an AS number for the aggregator.

This command is valid for BGP update messages only.

**Example** To use entry 3 of the route map called `myroute` to set the aggregator attribute to 43 10.10.0.3 in matching update messages, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# set aggregator as 43 10.10.0.3
```

To remove all aggregator attributes for entry 3 of the route map called `myroute`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# no set aggregator as
```

**Related commands** [route-map](#)  
[show route-map](#)

# set as-path

**Overview** Use this command to add an AS path set clause to a route map entry.

When a BGP update message matches the route map entry, the device prepends the specified Autonomous System Number (ASN) or ASNs to the update's AS path attribute.

The AS path attribute is a list of the autonomous systems through which the announcement for the prefix has passed. As prefixes pass between autonomous systems, each autonomous system adds its ASN to the beginning of the list. This means that the AS path attribute can be used to make routing decisions.

Use the **no** variant of this command to remove the set clause.

**Syntax** `set as-path prepend <1-65535> [<1-65535>]...`  
`no set as-path prepend [<1-65535> [<1-65535>]...]`

| Parameter                    | Description                                                                                    |
|------------------------------|------------------------------------------------------------------------------------------------|
| <code>prepend</code>         | Prepends the autonomous system path.                                                           |
| <code>&lt;1-65535&gt;</code> | The number to prepend to the AS path. If you specify multiple ASNs, separate them with spaces. |

**Mode** Route-map mode

**Usage notes** Use the **set as-path** command to specify an autonomous system path. By specifying the length of the AS-Path, the device influences the best path selection by a neighbor. Use the `prepend` parameter with this command to prepend an AS path string to routes increasing the AS path length.

This command is valid for BGP update messages only.

**Example** To use entry 3 of the route map called `myroute` to prepend ASN 8 and 24 to the AS path of matching update messages, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# set as-path prepend 8 24
```

**Related commands** [match as-path](#)  
[route-map](#)  
[show route-map](#)

**Command changes** Added to AlliedWare Plus prior to 5.4.6-1  
Version 5.4.7-2.1: BGP support added for x510 and x550 series  
Version 5.4.7-2.4: BGP support added for IE300 series

# set atomic-aggregate

**Overview** Use this command to add an atomic aggregate set clause to a route map entry.

When a BGP update message matches the route map entry, the device adds the atomic aggregate attribute to the update.

Use the **no** variant of this command to remove the set clause.

**Syntax** `set atomic-aggregate`  
`no set atomic-aggregate`

**Mode** Route-map Configuration

**Usage** This command is valid for BGP update messages only.

**Example** To use entry 3 of the route map called `rmap1` to add the atomic aggregator attribute to matching update messages, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set atomic-aggregate
```

**Related commands** [route-map](#)  
[show route-map](#)



# set comm-list delete

**Overview** Use this command to delete one or more communities from the community attribute of a BGP update message. Specify the communities to delete by specifying a community list. To create the community list, enter Global Configuration mode and use the [ip community-list](#) command.

When a BGP update message matches the route map entry, the device deletes the specified communities from the update's community attribute.

Use the **no** variant of this command to stop deleting the communities.

**Syntax** `set comm-list {<1-199>|<100-199>|<word>} delete`  
`no set comm-list {<1-199>|<100-199>|<word>} delete`

| Parameter | Description                     |
|-----------|---------------------------------|
| <1-99>    | Standard community-list number. |
| <100-199> | Expanded community-list number. |
| <word>    | Name of the Community-list.     |

**Mode** Route-map Configuration

**Usage** This command is valid for BGP update messages only.

**Example** To use entry 3 of the route map called `myroute` to delete the communities in community list 34 from matching update messages, use the commands:

```
awplus# configure terminal
awplus(config)# route-map myroute permit 3
awplus(config-route-map)# set comm-list 34 delete
```

**Related commands** [ip community-list](#)  
[match community](#)  
[route-map](#)  
[set community](#)  
[show route-map](#)

# set community

**Overview** Use this command to add a community set clause to a route map entry.

When a BGP update message matches the route map entry, the device takes one of the following actions:

- changes the update's community attribute to the specified value or values, or
- adds the specified community value or values to the update's community attribute, if you specify the **additive** parameter after specifying another parameter. or
- removes the community attribute from the update, if you specify the **none** parameter

Use the **no** variant of this command to remove the set clause.

**Syntax**

```
set community {[<1-65535>][AA:NN] [internet] [local-AS]
[no-advertise] [no-export] [additive]}

no set community {[AA:NN] [internet] [local-AS] [no-advertise]
[no-export] [additive]}

set community none

no set community none
```

| Parameter    | Description                                                                                                                                                                                                                                                                                                                                                         |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-65535>    | The AS number of the community as an integer not in AA:NN format.                                                                                                                                                                                                                                                                                                   |
| AA:NN        | The Autonomous System (AS) number of the community, in AA:NN format. AS numbers are assigned to the regional registries by the IANA ( <a href="http://www.iana.org">www.iana.org</a> ) and can be obtained from the registry in your region.<br>AA and NN are both integers from 1 to 65535.<br>AA is the AS number; NN is a value chosen by the ASN administrator. |
| local-AS     | The community of routes that must not be advertised to external BGP peers (this includes peers in other members' Autonomous Systems inside a BGP confederation).                                                                                                                                                                                                    |
| internet     | The community of routes that can be advertised to all BGP peers.                                                                                                                                                                                                                                                                                                    |
| no-advertise | The community of routes that must not be advertised to other BGP peers.                                                                                                                                                                                                                                                                                             |
| no-export    | The community of routes that must not be advertised outside a BGP confederation boundary (a standalone Autonomous System that is not part of a confederation should be considered a confederation itself).                                                                                                                                                          |

| Parameter | Description                                                                                                                                                                                                                       |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| none      | The device removes the community attribute from matching update messages.                                                                                                                                                         |
| additive  | The device adds the specified community value to the update message's community attribute, instead of replacing the existing attribute. By default this parameter is not included, so the device replaces the existing attribute. |

**Mode** Route-map Configuration

**Usage notes** This command is valid for BGP update messages only.

**Examples** To use entry 3 of the route map called `rmap1` to put matching routes into the no-advertise community, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community no-advertise
```

To use entry 3 of the route map called `rmap1` to put matching routes into several communities, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community 10:01 23:34 12:14
no-export
```

To use entry 3 of the route map called `rmap1` to put matching routes into a single AS community numbered 16384, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set community 16384 no-export
```

**Related commands**

- [match community](#)
- [route-map](#)
- [set aggregator](#)
- [set comm-list delete](#)
- [set extcommunity](#)
- [show route-map](#)

**Command changes**

- Added to AlliedWare Plus prior to 5.4.6-1
- Version 5.4.7-2.1: BGP support added for x510 and x550 series
- Version 5.4.7-2.4: BGP support added for IE300 series

# set dampening

**Overview** Use this command to add a route flap dampening set clause to a route map entry.

Also use the route map by specifying it in the command [bgp dampening route-map](#).

When a route matches the route map entry, the device enables route flap dampening for that route. If the set clause includes dampening parameter values, the device uses those values when dampening the matching route.

Use the **no** variant of this command to remove the set clause. This disables dampening on matching routes.

**Syntax**

```
set dampening
set dampening [<reachtime>]
set dampening <reachtime> [<reuse> <suppress> <maxsuppress>]
[<unreachtime>]
no set dampening
no set dampening [<reachtime>]
no set dampening <reachtime> [<reuse> <suppress> <maxsuppress>]
[<unreachtime>]
```

| Parameter   | Description                                                                                                                                                                                                                                                                                                                                        |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <reachtime> | <1-45><br>The time it takes, in minutes, for the route's instability penalty to halve if the route remains stable. The instability penalty is called the Figure of Merit (FoM). For example, if reachtime is 15, the FoM of a stable route halves over a 15 minute period, quarters over a 30 minute period, and so on. The default is 15 minutes. |
| <reuse>     | <1-20000><br>The value that the instability penalty (FoM) must reach for the device to use a suppressed route again. Once a route is suppressed, it remains suppressed until its FoM falls below this threshold. Reuse must not exceed suppress. The default is 750.                                                                               |
| <suppress>  | <1-20000><br>The instability penalty (FoM) at which the route is suppressed. Suppress must be greater than or equal to reuse. If suppress is less than 1000, a route is suppressed when it becomes unreachable for the first time. The default is 2000.                                                                                            |

| Parameter                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;maxsuppress&gt;</code> | <code>&lt;1-255&gt;</code><br>A number that is multiplied by reachtime to give the maximum time in minutes for which a suppressed route must remain stable in order to become unsuppressed. The lowest maxsuppress value of 1 gives a maximum suppression time of 1 x reachtime, and the highest maxsuppress value of 255 gives a maximum suppression time of 255 x reachtime.<br>For example, if reachtime is 15 and maxsuppress is 4, the route is unsuppressed after 60 minutes of stability even if its FoM still exceeds reuse. The default is 4. |
| <code>&lt;unreachtime&gt;</code> | <code>&lt;1-45&gt;</code><br>The time it takes, in minutes, for the route's instability penalty to halve if the route remains unstable. The default is 15 minutes.                                                                                                                                                                                                                                                                                                                                                                                     |

**Mode** Route-map Configuration

**Usage** The **suppress** value must be greater than or equal to the **reuse** value.  
Set the unreachability half-life time to be equal to, or greater than, reachability half-life time. The suppress-limit value must be greater than or equal to the reuse limit value.  
This command is valid for BGP routes only.

**Example** To use entry 24 of the route map called R1 to enable dampening of matching routes and set the dampening parameters, use the commands:

```
configure terminal
route-map R1 permit 24
set dampening 20 333 534 30
```

### Related commands

# set extcommunity

**Overview** Use this command to add an extended community set clause to a route map entry. A route map entry can have a route target extended community set clause, a site-of-origin extended community set clause, or both.

When a BGP update message matches the route map entry, the device sets the update's extended community attribute to the specified value or values.

Use the **no** variant of this command to remove the set clause.

**Syntax** `set extcommunity {rt|soo} <extcomm-number>`  
`no set extcommunity {rt|soo} [<extcomm-number>]`

| Parameter        | Description                                                                                                        |
|------------------|--------------------------------------------------------------------------------------------------------------------|
| rt               | Configure a route target extended community. This consists of routers that will receive matching routes.           |
| soo              | Configure a site-of-origin extended community. This consists of routers that will inject matching routes into BGP. |
| <extcomm-number> | The extended community number, in the format AA:NN or IPADD:N.                                                     |

**Mode** Route-map Configuration

**Usage notes** This command is valid for BGP update messages only.

**Examples** To use entry 3 of the route map called `rmap1` to set the route target extended community attribute to 06:01, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set extcommunity rt 06:01
```

To instead specify the extended community number in dotted decimal notation, use the command:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set extcommunity rt 0.0.0.6:01
```

To use entry 3 of the route map called `rmap1` to set the site-of-origin extended community attribute to 06:01, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set extcommunity soo 06:01
```

To instead specify the extended community number in dotted decimal notation, use the command:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set extcommunity soo 0.0.0.6:01
```

**Related  
commands**

[match community](#)  
[route-map](#)  
[set comm-list delete](#)  
[set community](#)  
[show route-map](#)

# set ip next-hop (route map)

**Overview** Use this command to add a next-hop set clause to a route map entry.

When a route or BGP update message matches the route map entry, the device sets the route's next hop to the specified IP address.

Use the **no** variant of this command to remove the set clause.

**Syntax** `set ip next-hop <ip-address>`  
`no set ip next-hop [<ip-address>]`

| Parameter                       | Description                                                  |
|---------------------------------|--------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code> | The IP address of the next hop, entered in the form A.B.C.D. |

**Mode** Route-map Configuration

**Usage notes** Use this command to set the next-hop IP address to the routes.

This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

**Example** To use entry 3 of the route map called `mymap` to give matching routes a next hop of 10.10.0.67, use the commands:

```
awplus# configure terminal
awplus(config)# route-map mymap permit 3
awplus(config-route-map)# set ip next-hop 10.10.0.67
```

**Related commands** [match ip next-hop](#)  
[route-map](#)  
[show route-map](#)



# set ipv6 next-hop

**Overview** Use this command to set a next hop-address.

Use the **no** variant of this command to delete an entry.

**Syntax** `set ipv6 next-hop {<ipv6-addr-global>|local <ipv6-addr>}`  
`no set ipv6 next-hop [<ipv6-addr-global>|local [<ipv6-addr>]]`

| Parameter          | Description                                                                     |
|--------------------|---------------------------------------------------------------------------------|
| <ipv6-addr-global> | The IPv6 global address of next hop. The IPv6 address uses the format X:X::X:X. |
| local              | Specifies that the address is local.                                            |
| <ipv6-addr>        | The IPv6 local address of next hop. The IPv6 address uses the format X:X::X:X.  |

**Mode** Route-map Configuration

**Usage notes** Use this command to set the next-hop IPv6 address to the routes.

This command is valid only for BGP.

**Examples** `awplus# configure terminal`  
`awplus(config)# route-map rmap1 permit 3`  
`awplus(config-route-map)# set ipv6 next-hop local`  
`fe80::203:47ff:fe97:66dc`  
`awplus(config-route-map)# no set ipv6 next-hop`

# set local-preference

**Overview** This command changes the default local preference value.

The local preference indicates the BGP local preference path attribute when there are multiple paths to the same destination. The path with the higher preference is chosen.

Use this command to define the preference of a particular path. The preference is sent to all routers and access servers in the local autonomous system.

The **no** variant of this command reverts to the default setting.

**Syntax** `set local-preference <pref-value>`  
`no set local-preference [<pref-value>]`

| Parameter                       | Description                                                                                 |
|---------------------------------|---------------------------------------------------------------------------------------------|
| <code>&lt;pref-value&gt;</code> | <0-4294967295> Configure local preference value. The default local preference value is 100. |

**Mode** Route-map Configuration

**Examples**

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set local-preference 2345555
awplus# configure terminal
awplus(config)# router bgp 100
awplus(config-route-map)# no set local-preference
```

**Related commands** For related Route Map commands:

[route-map](#)

[show route-map](#)

For related BGP commands:

[bgp default local-preference \(BGP only\)](#)

[neighbor route-map](#)

# set metric

**Overview** Use this command to add a metric set clause to a route map entry.

When a route or BGP update message matches the route map entry, the device takes one of the following actions:

- changes the metric (or for BGP, the MED attribute value) to the specified value, or
- adds or subtracts the specified value from the metric or MED attribute, if you specify + or - before the value (for example, to increase the metric by 2, enter +2)

Use the **no** variant of this command to remove the set clause.

**Syntax** `set metric {+<metric-value>|-<metric-value>|<metric-value>}`  
`no set metric [+<metric-value>|-<metric-value>|<metric-value>]`

| Parameter      | Description                                                                                                                 |
|----------------|-----------------------------------------------------------------------------------------------------------------------------|
| +              | Increase the metric or MED attribute by the specified amount.                                                               |
| -              | Decrease the metric or MED attribute by the specified amount.                                                               |
| <metric-value> | <0-4294967295><br>The new metric or MED attribute value, or the amount by which to increase or decrease the existing value. |

**Default** The default metric value for routes redistributed into OSPF and OSPFv3 is 20.

**Mode** Route-map Configuration

**Usage notes** For BGP, if you want the device to compare MED values in update messages from peers in different ASes, also enter the command [bgp always-compare-med](#). You do not need to enter this command if you only want the device to compare MED values in update messages from peers in the same AS, because it always does.

This command is valid for:

- OSPF routes
- routes in BGP update messages
- RIP routes.

Note that defining the OSPF metric in a route map supersedes the metric defined using a [redistribute \(OSPF\)](#) or a [redistribute \(IPv6 OSPF\)](#) command. For more information, see the [OSPFv3 Feature Overview and Configuration Guide](#) and the [OSPF Feature Overview and Configuration Guide](#).

**Examples** To use entry 3 of the route map called "rmap1" to give matching routes a metric of 600, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set metric 600
```

To use entry 3 of the route map called "rmap1" to increase the metric of matching routes by 2, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set metric +2
```

**Related commands**

- [match metric](#)
- [route-map](#)
- [show route-map](#)

# set metric-type

**Overview** Use this command to add a metric-type set clause to a route map entry.

When a route matches the route map entry, the device sets its route type to the specified value.

Use the **no** variant of this command to remove the set clause.

**Syntax** `set metric-type {type-1|type-2}`  
`no set metric-type [type-1|type-2]`

| Parameter | Description                                                       |
|-----------|-------------------------------------------------------------------|
| type-1    | Redistribute matching routes into OSPF as type-1 external routes. |
| type-2    | Redistribute matching routes into OSPF as type-2 external routes. |

**Mode** Route-map Configuration

**Usage notes** This command is valid for OSPF routes only.

**Example** To use entry 3 of the route map called `rmap1` to redistribute matching routes into OSPF as type-1 external routes, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set metric-type 1
```

**Related commands**

- [default-information originate](#)
- [redistribute \(OSPF\)](#)
- [match route-type](#)
- [route-map](#)
- [show route-map](#)

# set origin

**Overview** Use this command to add an origin set clause to a route map entry.

When a BGP update message matches the route map entry, the device sets its origin attribute to the specified value.

Use the **no** variant of this command to remove the set clause.

**Syntax** `set origin {egp|igp|incomplete}`  
`no set origin [egp|igp|incomplete]`

| Parameter  | Description                                      |
|------------|--------------------------------------------------|
| egp        | Learned from an exterior gateway protocol.       |
| igp        | Learned from a local interior gateway protocol.  |
| incomplete | Of unknown heritage, for example a static route. |

**Mode** Route-map Configuration

**Usage** This command is valid for BGP update messages only.

**Example** To use entry 3 of the route map called `rmap1` to give matching update messages an origin of `egp`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set origin egp
```

**Related commands** [match origin](#)  
[route-map](#)  
[show route-map](#)

# set originator-id

- Overview** Use this command to add an originator ID set clause to a route map entry.
- The originator ID is the router ID of the IBGP peer that first learned this route, either via an EBGP peer or by some other means such as importing it.
- When a BGP update message matches the route map entry, the device sets its originator ID attribute to the specified value.
- Use the **no** variant of this command to remove the set clause.

**Syntax** `set originator-id <ip-address>`  
`no set originator-id [<ip-address>]`

| Parameter                       | Description                                                    |
|---------------------------------|----------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code> | The IP address of the originator, entered in the form A.B.C.D. |

**Mode** Route-map Configuration

**Usage** This command is valid for BGP update messages only.

**Example** To use entry 3 of the route map called `rmap1` to give matching update messages an originator ID of `1.1.1.1`, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set originator-id 1.1.1.1
```

**Related commands** [route-map](#)  
[show route-map](#)

# set tag

**Overview** Use this command to add a tag set clause to a route map entry.

When a route matches the route map entry, the device sets its tag to the specified value when it redistributes the route into OSPF.

Use the **no** variant of this command to remove the set clause.

**Syntax** `set tag <tag-value>`  
`no set tag [<tag-value>]`

| Parameter                      | Description                                                             |
|--------------------------------|-------------------------------------------------------------------------|
| <code>&lt;tag-value&gt;</code> | <code>&lt;0-4294967295&gt;</code><br>Value to tag matching routes with. |

**Mode** Route-map Configuration

**Usage notes** This command is valid only when redistributing routes into OSPF.

**Example** To use entry 3 of the route map called `rmap1` to tag matching routes with the number 6, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set tag 6
```

**Related commands**

- [default-information originate](#)
- [redistribute \(OSPF\)](#)
- [match tag](#)
- [route-map](#)
- [show route-map](#)



# set weight

**Overview** Use this command to add a weight set clause to a route map entry.

The weight value assists in best path selection of BGP routes. It is stored with the route in the BGP routing table, but is not advertised to peers. When there are multiple routes with a common destination, the device uses the route with the highest weight value.

When a route matches the route map entry, the device sets its weight to the specified value.

Use the **no** variant of this command to remove the set clause.

**Syntax** `set weight <weight>`  
`no set weight [<weight>]`

| Parameter | Description                         |
|-----------|-------------------------------------|
| <weight>  | <0-4294967295><br>The weight value. |

**Mode** Route-map Configuration

**Usage** This command is valid for BGP routes only.

**Example** To use entry 3 of the route map called `rmap1` to give matching routes a weight of 60, use the commands:

```
awplus# configure terminal
awplus(config)# route-map rmap1 permit 3
awplus(config-route-map)# set weight 60
```

**Related commands** [route-map](#)  
[show route-map](#)

# show route-map

**Overview** Use this command to display information about one or all route maps.

**Syntax** `show route-map <map-name>`

| Parameter                     | Description                       |
|-------------------------------|-----------------------------------|
| <code>&lt;map-name&gt;</code> | A name to identify the route map. |

**Mode** User Exec and Privileged Exec

**Example** To display information about the route-map named `example-map`, use the command:

```
awplus# show route-map example-map
```

**Output** Figure 25-1: Example output from the **show route-map** command

```
route-map example-map, permit, sequence 1
 Match clauses:
 ip address prefix-list example-pref
 Set clauses:
 metric 100
route-map example-map, permit, sequence 200
 Match clauses:
 Set clauses:
```

**Related commands** [route-map](#)

# 26

# Policy-based Routing Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure policy-based routing.

For more information, see the [Policy-based Routing \(PBR\) Feature Overview and Configuration Guide](#).

- Command List**
- [“application-decision”](#) on page 1256
  - [“debug policy-based-routing”](#) on page 1258
  - [“ip policy-route”](#) on page 1259
  - [“ipv6 policy-route”](#) on page 1261
  - [“policy-based-routing”](#) on page 1263
  - [“policy-based-routing enable”](#) on page 1264
  - [“show ip pbr route”](#) on page 1265
  - [“show ipv6 pbr route”](#) on page 1267
  - [“show pbr rules”](#) on page 1269
  - [“show pbr rules brief”](#) on page 1274

# application-decision

**Overview** Use this command to select which method is used for the application decision.

**Syntax** `application-decision {once-only|continuous}`

| Parameter  | Description                                                                                                                                                                                                                                                     |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| once-only  | When a traffic flow reaches the PBR engine for the first time, whatever application has been set on that flow will be used to match against the PBR rules and a route selected. Subsequent updates to the flow's application will be ignored by the PBR engine. |
| continuous | Any time a traffic flow has its application updated by the DPI engine, the PBR engine will re-process the flow against all configured PBR rules, which may result in a new match and the traffic being directed over a different route than it was previously.  |

**Default** Application determination is set to **continuous**.

**Mode** Policy-based Routing Configuration

**Usage notes** When using a DPI engine, traffic flows through the device are periodically assigned an application by the DPI engine. The application assignment is then used when matching against PBR rules. The DPI engine may change its decision about a traffic flow over time, as more packets from the flow are analyzed. This command determines how the PBR engine utilizes the application decision made by DPI.

When set to **once-only**, only the initial application decision made by the DPI engine will be used when matching against PBR routes, and subsequent updates will be ignored.

When set to **continuous**, if the DPI engine re-classifies a traffic flow under a different application, the flow will be re-processed by the PBR engine, and may therefore match against a different PBR rule and take a different route than it was previously.

Once-only is intended for use with DPI learning enabled. Refer to the [SD-WAN Feature Overview and Configuration Guide](#) for examples.

**Example** To prevent the PBR engine from re-matching a traffic flow whenever the application decision is changed, use the following commands:

```
awplus(config)# policy-based-routing
awplus(config-pbr)# application-decision once-only
```

To allow the PBR engine to re-match traffic flows against PBR rules when the application decision changes, use the following commands:

```
awplus(config)# policy-based-routing
awplus(config-pbr)# application-decision continuous
```

**Related  
commands**   [ip policy-route](#)  
[ipv6 policy-route](#)

**Command  
changes**   Version 5.4.8-0.2: command added

# debug policy-based-routing

**Overview** Use this command to enable policy-based routing debugging. This will cause messages containing detailed debugging information to be displayed and logged at the "debugging" level.

Use the **no** variant of this command to disable policy-based routing debugging.

**Syntax** `debug policy-based-routing`  
`no debug policy-based-routing`

**Default** Policy-based routing debugging is disabled by default.

**Mode** Privileged Exec

**Examples** To enable policy-based routing debugging, use the command:

```
awplus# debug policy-based-routing
```

To disable policy-based routing debugging, use the command:

```
awplus# no debug policy-based-routing
```

**Related commands**

- [ip policy-route](#)
- [ipv6 policy-route](#)
- [policy-based-routing](#)
- [show ip pbr route](#)
- [show ipv6 pbr route](#)

# ip policy-route

**Overview** Use this command to configure IP policy routes. These routes specify how the device will route traffic from specified applications and entities. You can specify the route's next-hop by specifying the egress interface, or by specifying the next-hop device's IP address (except on dynamic interfaces such as PPPoE). You can also list alternative next-hops to use if your first choice is down.

You can also specify the pseudo interface Null. Null should be the last nexthop specified, as this will drop packets when used as the nexthop.

Use the **no** variant of this command to remove a policy route.

**Syntax** `ip policy-route [<1-500>] [match <application-name>] [from <source-entity>] [to <destination-entity>] nexthop {<interface-list>|<ip-add-list>}`  
`no ip policy-route <1-500>`

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-500>              | The policy route ID number.<br>If you do not specify an ID number, the device assigns the new policy route the next available number, in multiples of 10. For example, if the highest numbered policy route is 81, the next policy route would be given an ID of 90.<br>Policy routes are checked in order of ID number, starting with the lowest ID number. The device applies the policy route as soon as it finds a matching route; it does not check the remaining policy routes. |
| <application-name>   | An application name.<br>You can use the tab key to auto-complete application names.                                                                                                                                                                                                                                                                                                                                                                                                   |
| <source-entity>      | A source entity name.<br>You can use the tab key to auto-complete entity names.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <destination-entity> | A destination entity name.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <interface-list>     | The name of the egress interface or interfaces. You can list up to 8 interfaces per policy route; the device sends the traffic out the first interface in the list that is up.                                                                                                                                                                                                                                                                                                        |
| <ip-add-list>        | The IP address of the next-hop. You can list up to 8 next-hop addresses per policy route; the device sends the traffic to the first address in the list that is reachable. Do not use this when the next-hop is on a dynamic interface (e.g. PPPoE); specify the interface name instead.                                                                                                                                                                                              |

**Default** No policy routes

**Mode** Policy-based Routing Configuration

**Usage notes** You must specify at least one of the **match**, **from** or **to** parameters. Packets will be routed to the specified next-hop if they match the application, come from the source entity, and are destined for the destination entity.

Before creating a policy route, you need to create the application and entities that specify the traffic you want to route. To create an application, use the [application](#) command. To create entities, use the [zone](#), [network \(zone\)](#), and [host \(network\)](#) commands. To see existing applications and entities, use the [show application](#) and [show entity](#) commands.

**Examples** To create a policy route to route traffic that matches an application called 'voice', comes from the entity called 'inside', and is destined for the entity called 'outside', use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ip policy-route 10 match voice from inside
to outside nexthop 10.37.236.65
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ip policy-route 10
```

To route the above traffic via ppp0 if ppp0 is up, or ppp1 if ppp0 is down, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ip policy-route 20 match voice from inside
to outside nexthop ppp0 ppp1
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ip policy-route 20
```

**Related commands**

- [policy-based-routing](#)
- [policy-based-routing enable](#)
- [show application](#)
- [show entity](#)
- [show ip pbr route](#)

**Command changes** Version 5.4.8-0.2: number of routes increased, null interface added



# ipv6 policy-route

**Overview** Use this command to configure IPv6 policy routes. These routes specify how the device will route traffic from specified applications and entities. You can specify the route's next-hop by specifying the egress interface, or by specifying the next-hop device's IPv6 address (except on dynamic interfaces such as PPPoE). You can also list alternative next-hops to use if your first choice is down.

You can also specify the pseudo interface Null. Null should be the last nexthop specified, as this will drop packets when used as the nexthop.

Use the **no** variant of this command to remove a policy route.

**Syntax** `ipv6 policy-route [<1-500>] [match <application-name>] [from <source-entity>] [to <destination-entity>] nexthop {<interface-list>|<ipv6-add-list>}`  
`no ipv6 policy-route <1-500>`

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-500>              | The policy route ID number.<br>If you do not specify an ID number, the device assigns the new policy route the next available number, in multiples of 10. For example, if the highest numbered policy route is 81, the next policy route would be given an ID of 90.<br>Policy routes are checked in order of ID number, starting with the lowest ID number. The device applies the policy route as soon as it finds a matching route; it does not check the remaining policy routes. |
| <application-name>   | An application name.<br>You can use the tab key to auto-complete application names.                                                                                                                                                                                                                                                                                                                                                                                                   |
| <source-entity>      | A source entity name.<br>You can use the tab key to auto-complete entity names.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <destination-entity> | A destination entity name.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <interface-list>     | The name of the egress interface or interfaces. You can list up to 8 interfaces per policy route; the device sends the traffic out the first interface in the list that is up.                                                                                                                                                                                                                                                                                                        |
| <ipv6-add-list>      | The IPv6 address of the next-hop, specified in the form X:X::X:X. You can list up to 8 next-hop addresses per policy route; the device sends the traffic to the first address in the list that is reachable.<br>Do not use this when the next-hop is on a dynamic interface (e.g. PPPoE); specify the interface name instead.                                                                                                                                                         |

**Default** No policy routes

**Mode** Policy-based Routing Configuration

**Usage notes** You must specify at least one of the **match**, **from** or **to** parameters. Packets will be routed to the specified next-hop if they match the application, come from the source entity, and are destined for the destination entity.

Before creating a policy route, you need to create the application and entities that specify the traffic you want to route. To create an application, use the [application](#) command. To create entities, use the [zone](#), [network \(zone\)](#), and [host \(network\)](#) commands. To see existing applications and entities, use the [show application](#) and [show entity](#) commands.

**Examples** To create a policy route to route traffic that matches an application called 'voice', comes from the entity called 'inside', and is destined for the entity called 'outside', use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ipv6 policy-route 10 match voice from
inside to outside nexthop 2001:100::1
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ipv6 policy-route 10
```

To route the above traffic via ppp0 if ppp0 is up, or ppp1 if ppp0 is down, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ipv6 policy-route 20 match voice from
inside to outside nexthop ppp0 ppp1
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ipv6 policy-route 20
```

**Related commands**

- [policy-based-routing](#)
- [policy-based-routing enable](#)
- [show application](#)
- [show entity](#)
- [show ipv6 pbr route](#)

**Command changes** Version 5.4.8-0.2: number of routes increased, null interface added

# policy-based-routing

**Overview** Use this command to enter Policy-based-routing mode. Policy-based routing lets you determine how the device will route traffic from specified applications and entities.

Use the **no** variant of this command to remove the whole policy-based routing configuration.

**Syntax** `policy-based-routing`  
`no policy-based-routing`

**Mode** Global configuration

**Usage** Once you have entered policy-based-routing mode, use the [policy-based-routing enable](#) command to turn on policy-based routing, and the [ip policy-route](#) or [ipv6 policy-route](#) commands to create policy routes.

**Example** To enter policy-based-routing mode, use the commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)#
```

**Related commands** [ip policy-route](#)  
[ipv6 policy-route](#)  
[policy-based-routing enable](#)

# policy-based-routing enable

**Overview** Use this command to enable policy-based routing (PBR). Policy-based routing lets you determine how the device will route traffic from specified applications and entities.

Use the **no** variant of this command to disable policy-based routing.

**Syntax** `policy-based-routing enable`  
`no policy-based-routing enable`

**Default** Policy-based routing is disabled by default

**Mode** Policy-based Routing Configuration

**Examples** To enable policy-based routing use the following commands.

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
```

To disable policy-based routing use the following commands.

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no policy-based-routing enable
```

**Related commands** [ip policy-route](#)  
[ipv6 policy-route](#)

# show ip pbr route

**Overview** Use this command to display the installed IPv4 routes for policy-based routing.

**Syntax** `show ip pbr route [<1-500>]`

| Parameter | Description                                                                                                                                                                                                                 |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-500>   | The policy route ID. If you specify a policy route ID, the output only lists routes for that ID. If you do not specify an ID, the output also lists the conventional static and dynamic routes, in the table called "main". |

**Mode** User Exec and Privileged Exec

**Usage notes** If you do not specify a policy routeID, the output starts by listing the ordinary static and dynamic routes, in a table called "main".

**Example** To show all the IPv4 routes, use the following command:

```
awplus# show ip pbr route
```

**Output** Figure 26-1: Example output from **show ip pbr route**

```
awplus#show ip pbr route
Route table: main
 10.33.11.0/24 via 10.37.236.65, eth1
 10.37.236.64/27 is directly connected, eth1
 172.31.0.0/17 is directly connected, eth2
 192.168.1.0/24 is directly connected, eth2

Route table: policy-route 10

Route table: policy-route 20
 default via 10.37.236.65, ppp0
```

If you do not specify a policy routeID, the output starts by listing the ordinary static and dynamic routes, in the route table called "main".

Then it lists the routes for each policy route.

For each route, the output lists the route's next-hop IP address and/or the next-hop interface.

**Example** To show only the routes for policy route 20, use the following command:

```
awplus# show ip pbr route 20
```

**Output** Figure 26-2: Example output from **show ip pbr route** for a specified policy route

```
awplus#show ip pbr route 20

Route table: policy-route 20
 default via 10.37.236.65, ppp0
```

For each route, the output lists the route's next-hop IP address and/or the next-hop interface.

**Related commands** [ip policy-route](#)  
[policy-based-routing](#)

**Command changes** Version 5.4.8-0.2: Policy route ID increased from 128 to 500

# show ipv6 pbr route

**Overview** Use this command to display the installed IPv6 routes for policy-based routing.

**Syntax** `show ipv6 pbr route [<1-128>]`

| Parameter | Description                                                                                                                                                                                                             |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-128>   | The policy route ID. If you specify a policy route ID, the output only lists routes for that ID. If you do not specify an ID, the output also lists the ordinary static and dynamic routes, in the table called "main". |

**Mode** User Exec and Privileged Exec

**Usage** If you do not specify a policy routeID, the output starts by listing the ordinary static and dynamic routes, in a table called "main".

**Example** To show all the IPv6 routes, use the following command:

```
awplus# show ipv6 pbr route
```

**Output** Figure 26-3: Example output from **show ipv6 pbr route**

```
awplus#show ipv6 pbr route
Route table: main
 2001:100::/64 dev eth1
 fe80::/64 dev eth1

Route table: policy-route 10

Route table: policy-route 20
 default via 2001:100::2, eth1
```

If you do not specify a policy routeID, the output starts by listing the ordinary static and dynamic routes, in the route table called "main".

Then it lists the routes for each policy route.

For each route, the output lists the route's next-hop IPv6 address and/or the next-hop interface.

**Example** To show only the routes for policy-route 20, use the following command:

```
awplus# show ip pbr route 20
```

**Output** Figure 26-4: Example output from **show ipv6 pbr route** for a specified policy route

```
awplus#show ipv6 pbr route 20

Route table: policy-route 20
 default via 2001:100::2, eth1
```

For each route, the output lists the route's next-hop IPv6 address and/or the next-hop interface.

**Related commands** [ipv6 policy-route](#)  
[policy-based-routing](#)



# show pbr rules

**Overview** Use this command to display the configured IPv4 and IPv6 policy routes. It also shows the validity of the policy routes.

**Syntax**

```
show pbr rules
show pbr rules <rule-id>
show pbr rules profile <profile-name>
show pbr rules group <group-name>
```

| Parameter      | Description                                                                                                                                                                                  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <rule-id>      | The policy route ID. If you specify a policy route ID, the output only lists configuration and status for this specified rule.                                                               |
| <profile-name> | The Link Health Monitoring profile name. If you specify an existing Link Health Monitoring performance profile name, the output only lists profile configuration for this specified profile. |
| <group-name>   | The Link Health Monitoring group name. If you specify an existing Link Health Monitoring group name, the output only lists group configuration for this specified profile.                   |

**Mode** User Exec and Privileged Exec

**Example** To show information about the policy routes, use the following command:

```
awplus# show pbr rules
```

To show information about the policy route rule with the rule ID of '1', use the following command:

```
awplus# show pbr rules 1
```

To show information about the Link Health Monitoring profile with the profile name of 'profile1', use the following command:

```
awplus# show pbr rules profile profile1
```

To show information about the Link Health Monitoring group with the profile name of 'group1', use the following command:

```
awplus# show pbr rules group group1
```

**Output** Figure 26-5: Example output from **show pbr rules**

```
awplus#show pbr rules
Statistics:

Route table usage: 1/500
Total number of configured PBR-rules = 1

PBR-Rule 1

Active: Yes
Match: sip
From: LAN
To: any
Profile: PROFILE1
 latency bad above: 300 ms
 latency good below: - ms
 jitter bad above: - ms
 jitter good below: - ms
 pktloss bad above: - %
 pktloss good below: - %
Group: GROUP1
 Member: 10
 next-hop: 172.16.10.1
 probe: PROBE10
 latency: 401 ms
 jitter: 0 ms
 pktloss: 0.0 %
 Member: 20
 next-hop: 172.16.20.1
 probe: PROBE20
 latency: 400 ms
 jitter: 0 ms
 pktloss: 0.0 %
Last Change:
 Current Nexthop: 172.16.10.1
 Previous Nexthop: -
 Change Time: 22 Nov 2017 13:57:48
 Causes: Rx probe 'PROBE10', latency (401>300) ms
 Decision: only available link
Change Count: 1
```

Figure 26-6: Example output from **show pbr rules 1**

```
awplus#show pbr rules 1
PBR-Rule 1

Active: Yes
Match: sip
From: LAN
To: any
Profile: PROFILE1
 latency bad above: 300 ms
 latency good below: - ms
 jitter bad above: - ms
 jitter good below: - ms
 pktloss bad above: - %
 pktloss good below: - %
Group: GROUP1
 Member: 10
 next-hop: 172.16.10.1
 probe: PROBE10
 latency: 401 ms
 jitter: 0 ms
 pktloss: 0.0 %
 Member: 20
 next-hop: 172.16.20.1
 probe: PROBE20
 latency: 400 ms
 jitter: 0 ms
 pktloss: 0.0 %
Last Change:
 Current Nexthop: 172.16.10.1
 Previous Nexthop: -
 Change Time: 22 Nov 2017 13:57:48
 Causes: Rx probe 'PROBE10', latency (401>300) ms
 Decision: only available link
Change Count: 1
```

Figure 26-7: Example output from **show pbr rules profile profile1**

```
awplus#show pbr rules profile profile1
Profile: profile1
 latency bad above: 300 ms
 latency good below: - ms
 jitter bad above: - ms
 jitter good below: - ms
 pktloss bad above: - %
 pktloss good below: - %
```

Figure 26-8: Example output from **show pbr rules group group1**

```
awplus#show pbr rules group group1
Group: group1
 Member: 10
 next-hop: 172.16.10.1
 probe: PROBE10
 latency: 401 ms
 jitter: 0 ms
 pktloss: 0.0 %
 Member: 20
 next-hop: 172.16.20.1
 probe: PROBE20
 latency: 400 ms
 jitter: 0 ms
 pktloss: 0.0 %
```

Table 26-1: Parameters in the output from **show pbr rules**

| Parameter                            | Description                                                                                                                                                                                    |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Total number of configured PBR-rules | The number of PBR rules currently configured. This includes both conventional PBR policy-routes and Link Health Monitoring IP policy-routes, regardless of whether the rules are valid or not. |
| PBR-Rule                             | The PBR rule ID which the following statistics and configuration are associated with.                                                                                                          |
| Active                               | Whether the rule is active or not.                                                                                                                                                             |
| Match                                | The name of an application. Packets will be routed to the specified next hop if they match this application, come from the source entity, and are destined for the destination entity.         |
| From                                 | The name of the source entity. Packets will be routed to the specified next hop if they match the application, come from this source entity, and are destined for the destination entity.      |
| To                                   | The name of the destination entity. Packets will be routed to the specified next hop if they match the application, come from the source entity, and are destined for this destination entity. |
| Profile                              | The name of the Link Health Monitoring profile associated with this Link Health Monitoring PBR policy-route.                                                                                   |
| bad above,<br>good below             | The configured threshold for this specific rule. There are fields for latency, jitter, and packet loss. If this field has a value of "-", then the threshold has not been configured.          |
| Group                                | The name of the Link Health Monitoring group associated with this Link Health Monitoring PBR policy-route.                                                                                     |

Table 26-1: Parameters in the output from **show pbr rules** (cont.)

| Parameter        | Description                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Member           | The ID of the Link Health Monitoring member associated with this Link Health Monitoring group.                                                        |
| Nexthop          | The IPv4 or IPv6 address of the next-hop or the egress interface. There can be up to 8 next-hops per policy route.                                    |
| probe            | The Link Health Monitoring probe associated with the Link Health Monitoring group member.                                                             |
| latency          | The latency of the probe associated with the Link Health Monitoring member.                                                                           |
| jitter           | The jitter of the probe associated with the Link Health Monitoring member.                                                                            |
| packet loss      | The packet loss of the probe associated with the Link Health Monitoring member.                                                                       |
| Current Nexthop  | The chosen nexthop for traffic matching the Link Health Monitoring PBR policy-route.                                                                  |
| Previous Nexthop | The previously chosen nexthop prior to failover. If a failover hasn't occurred on this setup, there is no previous nexthop. This is indicated by "-". |
| Change Time      | The time at which the current nexthop was chosen. This will change if a failover occurs, or at boot.                                                  |
| Causes           | The event that caused the last failover.                                                                                                              |
| Decision         | The reason why the current nexthop was chosen.                                                                                                        |
| Change Count     | The number of times the chosen nexthop has changed. This counter will increment any time a link failover occurs.                                      |

**Related commands**

- [ip policy-route](#)
- [ipv6 policy-route](#)
- [policy-based-routing](#)
- [show ip pbr route](#)
- [show ipv6 pbr route](#)

**Command changes**

- Version 5.4.8-0.2: new parameters for profiles and groups added
- Version 5.4.8-1.1: up to 500 route table entries supported

# show pbr rules brief

**Overview** Use this command to show a summary of all PBR rules. It also indicates, by the presence or absence of the nexthop field, which nexthop to route to.

**Syntax** show pbr rules brief

**Mode** User Exec and Privileged Exec

**Example** To show information about the policy routes, use the following command:

```
awplus# show pbr rules brief
```

**Output** Figure 26-9: Example output from **show pbr rules brief**

```
awplus#show pbr rules brief
Policy based routing is enabled
Route table usage: 2/500
* - No route table available for the rule - see "show ip pbr
route"
Rule Match From To Valid Nexthop

10 any entities.any entities.outside Yes 10.10.20.2
20 udp any any Yes 2001:100::2
```

Table 26-2: Parameters in the output from **show pbr rules brief**

| Parameter | Description                                                                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule      | The policy route ID number.<br>Policy routes are checked in order of ID number, starting with the lowest ID number. The device applies the policy route as soon as it finds a matching route; it does not check the remaining policy routes. |
| Match     | The name of an application.<br>Packets will be routed to the specified next hop if they match this application, come from the source entity, and are destined for the destination entity.                                                    |
| From      | The name of the source entity.<br>Packets will be routed to the specified next hop if they match the application, come from this source entity, and are destined for the destination entity.                                                 |
| To        | The name of the destination entity.<br>Packets will be routed to the specified next hop if they match the application, come from the source entity, and are destined for this destination entity.                                            |

Table 26-2: Parameters in the output from **show pbr rules brief** (cont.)

| Parameter | Description                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------|
| Valid     | Whether the application and entities are valid.                                                                    |
| Nexthop   | The IPv4 or IPv6 address of the next-hop or the egress interface. There can be up to 8 next-hops per policy route. |

**Related commands** [show pbr rules](#)

**Command changes** Version 5.4.8-0.2: command added  
Version 5.4.8-1.1: up to 500 route table entries supported

# 27

# SD-WAN Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure SD-WAN.

For more information, see the [SD-WAN Feature Overview and Configuration Guide](#).

- Command List**
- ["application-decision"](#) on page 1278
  - ["consecutive probe loss"](#) on page 1280
  - ["debug linkmon"](#) on page 1282
  - ["destination \(linkmon-probe\)"](#) on page 1284
  - ["dscp \(linkmon-probe\)"](#) on page 1286
  - ["egress interface \(linkmon-probe\)"](#) on page 1287
  - ["enable \(linkmon-probe\)"](#) on page 1288
  - ["interval \(linkmon-probe\)"](#) on page 1289
  - ["ip policy-route"](#) on page 1290
  - ["ip-version \(linkmon-probe\)"](#) on page 1292
  - ["ipv6 policy-route"](#) on page 1293
  - ["jitter"](#) on page 1295
  - ["latency"](#) on page 1297
  - ["linkmon group"](#) on page 1299
  - ["linkmon probe-history"](#) on page 1300
  - ["linkmon probe"](#) on page 1302
  - ["linkmon profile"](#) on page 1304
  - ["load-balancing"](#) on page 1305
  - ["member \(linkmon-group\)"](#) on page 1306



- [“pktloss”](#) on page 1308
- [“preference”](#) on page 1310
- [“sample-size \(linkmon-probe\)”](#) on page 1312
- [“show debugging linkmon”](#) on page 1313
- [“show linkmon probe”](#) on page 1314
- [“show linkmon probe-history”](#) on page 1317
- [“show pbr rules”](#) on page 1319
- [“show pbr rules brief”](#) on page 1324
- [“size \(linkmon-probe\)”](#) on page 1326
- [“source \(linkmon-probe\)”](#) on page 1327
- [“url \(linkmon-probe\)”](#) on page 1328

# application-decision

**Overview** Use this command to select which method is used for the application decision.

**Syntax** `application-decision {once-only|continuous}`

| Parameter  | Description                                                                                                                                                                                                                                                     |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| once-only  | When a traffic flow reaches the PBR engine for the first time, whatever application has been set on that flow will be used to match against the PBR rules and a route selected. Subsequent updates to the flow's application will be ignored by the PBR engine. |
| continuous | Any time a traffic flow has its application updated by the DPI engine, the PBR engine will re-process the flow against all configured PBR rules, which may result in a new match and the traffic being directed over a different route than it was previously.  |

**Default** Application determination is set to **continuous**.

**Mode** Policy-based Routing Configuration

**Usage notes** When using a DPI engine, traffic flows through the device are periodically assigned an application by the DPI engine. The application assignment is then used when matching against PBR rules. The DPI engine may change its decision about a traffic flow over time, as more packets from the flow are analyzed. This command determines how the PBR engine utilizes the application decision made by DPI.

When set to **once-only**, only the initial application decision made by the DPI engine will be used when matching against PBR routes, and subsequent updates will be ignored.

When set to **continuous**, if the DPI engine re-classifies a traffic flow under a different application, the flow will be re-processed by the PBR engine, and may therefore match against a different PBR rule and take a different route than it was previously.

Once-only is intended for use with DPI learning enabled. Refer to the [SD-WAN Feature Overview and Configuration Guide](#) for examples.

**Example** To prevent the PBR engine from re-matching a traffic flow whenever the application decision is changed, use the following commands:

```
awplus(config)# policy-based-routing
awplus(config-pbr)# application-decision once-only
```

To allow the PBR engine to re-match traffic flows against PBR rules when the application decision changes, use the following commands:

```
awplus(config)# policy-based-routing
awplus(config-pbr)# application-decision continuous
```

**Related  
commands**   [ip policy-route](#)  
[ipv6 policy-route](#)

**Command  
changes**   Version 5.4.8-0.2: command added

# consecutive probe loss

**Overview** Use this command within a specific link performance profile to configure the allowable consecutive probe loss thresholds of probes that use that performance profile.

Use the **no** variant of this command to delete a consecutive probe loss threshold.

**Syntax**

```
consecutive-probe-loss bad-when <consecutive-probe-losses>
consecutive-probe-loss good-when <consecutive-probe-successes>
consecutive-probe-loss unreachable-when
<consecutive-probe-losses>
no consecutive-probe-loss bad-when
no consecutive-probe-loss good-when
no consecutive-probe-loss unreachable-when
```

| Parameter                                      | Description                                                                                                                                      |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| bad-when<br><consecutive-probe-losses>         | The number of probes that must be lost consecutively, at which point the associated link is considered to be bad, in a range of <1-100>.         |
| good-when<br><consecutive-probe-successes>     | The number of probes that must succeed consecutively, at which point the associated link is considered to be good, in a range of <1-100>.        |
| unreachable-when<br><consecutive-probe-losses> | The number of probes that must be lost consecutively, at which point the associated link is considered to be unreachable, in a range of <1-100>. |

**Default** The performance profile is disabled.

**Mode** Linkmon Profile Configuration

**Usage notes** These setting are all optional.

The **bad-when** parameter is used to set the thresholds where if the number of probe replies that have been lost consecutively is equal to or above this value, then that nexthop is considered bad. If **bad-when** is not configured, this metric will never result in a nexthop being considered bad.

The **unreachable-when** parameter is used to set the thresholds where if the number of probe replies that have been lost consecutively is equal to or above this value, then that nexthop is considered unreachable or down. If **unreachable-when** is not configured, this metric will never result in a nexthop being considered unreachable.

The **good-when** parameter is used to state the thresholds where if the number of probe replies that have been successfully received consecutively is equal to or above this value, then that nexthop is considered good. If **good-when** is not

configured, then when a nexthop is considered bad or unreachable due to this metric, the first successful probe result will consider the nexthop as good.

**Example** To configure the point at or above which consecutive probe loss is unacceptable to be 10, the point at or above which consecutive probe success is acceptable to be 5, and the point at or above which consecutive probe loss indicates the destination is unreachable to be 15 for performance profile named "profile0", use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon profile profile0
awplus(config-linkmon-profile)# consecutive-probe-loss
bad-when 10
awplus(config-linkmon-profile)# consecutive-probe-loss
good-when 5
awplus(config-linkmon-profile)# consecutive-probe-loss
unreachable-when 15
```

To delete consecutive-probe-loss thresholds in performance profile "profile0", use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon profile profile0
awplus(config-linkmon-profile)# no consecutive-probe-loss
bad-when
awplus(config-linkmon-profile)# no consecutive-probe-loss
good-when
awplus(config-linkmon-profile)# no consecutive-probe-loss
unreachable-when
```

**Command  
changes**

Version 5.4.8-1.1: command added

Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# debug linkmon

**Overview** Use this command to enable Link Health Monitoring debugging.  
Use the **no** variant of this command to disable Link Health Monitoring debugging.

**Syntax**

```
debug linkmon
[probe|group|ip-address|interface|pbr-group|trigger]

no debug linkmon
[probe|group|ip-address|interface|pbr-group|trigger]

debug linkmon probe name <name>
no debug linkmon probe name <name>

debug linkmon group name <name>
no debug linkmon group name <name>
```

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| probe      | Link Health Monitoring probe.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| group      | Link Health Monitoring group.                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| ip-address | IP addresses that are of interest to Link Health Monitoring.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| interface  | Interfaces that are of interest to Link Health Monitoring.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| pbr-group  | This debug option will show debugging of policy-based routing Link Health Monitoring groups. Policy-based routing rules without an explicit Link Health Monitoring configuration will internally create Link Health Monitoring groups that are not visible from the Link Health Monitoring api/cli externally (apart from debug). The names for these groups are prefixed with 'pbr'. Their relationship to policy-based routing rules can be seen with policy-based routing debug enabled. |
| trigger    | This debug option will show debugging for Link Health Monitoring triggers.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <name>     | The name identifying a Link Health Monitoring probe or Link Health Monitoring group.                                                                                                                                                                                                                                                                                                                                                                                                        |

**Default** No debugging is enabled.

**Mode** Privileged Exec

**Usage notes** If **probe** is specified, then debug related to all Link Health Monitoring probes is enabled.  
  
If **probe name <name>** is specified, then debug related to the named Link Health Monitoring probe is enabled.  
  
If **group** is specified, then debug related to all Link Health Monitoring groups is enabled.

If **group name** <name> is specified, then debug related to the named Link Health Monitoring group is enabled.

If **ip-address** is specified, then debug related to configuration of IP addresses that are of interest to Link Health Monitoring are enabled. These IP addresses could influence Link Health Monitoring group members being considered up/down.

If **interface** is specified, then debug related to up/down state of Link Health Monitoring is enabled.

If **trigger** is specified, then debug related to Link Health Monitoring triggers is enabled.

**Example** To enable debugging on the Link Health Monitoring probe 'probe1', use the following command:

```
awplus# debug linkmon probe name probe1
```

To enable debugging on all Link Health Monitoring probes, use the following command:

```
awplus# debug linkmon probe
```

To enable debugging on all Link Health Monitoring groups, use the following command:

```
awplus# debug linkmon group
```

To disable debugging on all Link Health Monitoring probes, use the following command:

```
awplus# no debug linkmon probe
```

To disable debugging on all Link Health Monitoring groups, use the following command:

```
awplus# no debug linkmon group
```

**Related commands** [linkmon probe](#)  
[show debugging linkmon](#)

**Command changes** Version 5.4.8-0.2: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# destination (linkmon-probe)

**Overview** Use this command to set the destination of a Link Health Monitoring probe. This is a required configuration option for probes.

Use the **no** variant of this command to remove the destination of a probe.

**Syntax** `destination {<ip-address>|ds-lite|<fqdn>}`  
`no destination`

| Parameter    | Description                                                                                                                                              |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-address> | The destination of the probe, an IPv4 or IPv6 IP address.                                                                                                |
| ds-lite      | The destination of the probe, the DS-Lite AFTR address.                                                                                                  |
| <fqdn>       | The destination of the probe, an FQDN (fully qualified domain name). The IP address of the FQDN will be automatically resolved by the DNS on the device. |

**Mode** Linkmon ICMP Probe Configuration

**Example** To set the destination of a probe named 'probe1' to 192.168.2.200, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# destination 192.168.2.200
```

To set the destination of a probe named 'probe1' to 2001:db8:a0b:12f0::1, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# destination
2001:db8:a0b:12f0::1
```

To set the destination of a probe named 'probe1' to the DS-Lite AFTR address, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# destination ds-lite
```

To set the destination of a probe named 'probe1' to the FQDN of "google.com", use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# destination google.com
```

To remove the destination of a probe named 'probe1', use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# no destination
```



**Related commands** [linkmon probe](#)

**Command changes** Version 5.4.8-1.1: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

## dscp (linkmon-probe)

**Overview** Use this command to set the DSCP value of packets used for Link Health Monitoring probes.

Use the **no** variant of this command to set it back to the default.

**Syntax** `dscp <dscp-value>`  
`no dscp`

| Parameter                       | Description                                                              |
|---------------------------------|--------------------------------------------------------------------------|
| <code>&lt;dscp-value&gt;</code> | The DSCP value for the probe packet in range <code>&lt;0-63&gt;</code> . |

**Default** The default DSCP value is 0.

**Mode** Linkmon ICMP Probe Configuration

**Example** To set the DSCP of a probe named 'probe1' to 10, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# dscp 10
```

To set the DSCP of a probe named 'probe1' back to default, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# no dscp
```

**Related commands** [linkmon probe](#)

**Command changes** Version 5.4.8-1.1: command added

Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# egress interface (linkmon-probe)

**Overview** Use this command to force a Link Health Monitoring probe to egress out of a specific interface.

Use the **no** variant of this command to return interface selection back to the default behavior.

**Syntax** `egress interface <interface>`  
`no egress interface`

| Parameter                      | Description                                                                                                                                   |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;interface&gt;</code> | The name of the egress interface for the probe. The specified egress interface needs to be locally configured and in an up and running state. |

**Default** No egress interface is defined by default. The egress interface will be selected using standard routing behavior to reach the probe's destination.

**Mode** Linkmon HTTP Probe Configuration, or Linkmon ICMP Probe Configuration

**Example** To set the egress interface for a probe named 'probe1' to 'tunnel2', use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# egress interface tunnel2
```

To set the egress interface for a probe named 'probe1' back to the default, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# no egress interface
```

**Command changes** Version 5.4.8-1.1: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# enable (linkmon-probe)

**Overview** Use this command to enable individual Link Health Monitoring probes. When a probe is enabled, it will begin transmitting, processing, and storing results.

Use the **no** variant of this command to disable a probe.

**Syntax** enable  
no enable

**Default** Disabled

**Mode** Linkmon HTTP Probe Configuration, or Linkmon ICMP Probe Configuration

**Example** To enable a probe named 'probe1', use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# enable
```

To disable a probe named 'probe1', use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# no enable
```

**Related commands** [linkmon probe](#)

**Command changes** Version 5.4.8-1.1: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# interval (linkmon-probe)

**Overview** Use this command to set the interval between Link Health Monitoring probe packets.

Use the **no** variant of this command to set the interval back to the default.

**Syntax** `interval <probe-interval>`  
`no interval`

| Parameter                           | Description                                                                                                                                                           |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;probe-interval&gt;</code> | The gap between probes being transmitted. For ICMP probes, this is a range of 100-10000 milliseconds. For HTTP probes, this is a range of 30000-3600000 milliseconds. |

**Default** For ICMP probes, the default interval is 1000 milliseconds. For HTTP probes, the default interval is 60000 milliseconds.

**Mode** Linkmon HTTP Probe Configuration, or Linkmon ICMP Probe Configuration

**Example** To set the interval of a probe named 'probe1' to 100, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# interval 100
```

To set the interval of a probe named 'probe1' back to default, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# no interval
```

**Related commands** [linkmon probe](#)

**Command changes** Version 5.4.8-1.1: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# ip policy-route

**Overview** Use this command to configure IP policy routes. These routes specify how the device will route traffic from specified applications and entities. You can specify the route's next-hop by specifying the egress interface, or by specifying the next-hop device's IP address (except on dynamic interfaces such as PPPoE). You can also list alternative next-hops to use if your first choice is down.

You can also specify the pseudo interface Null. Null should be the last nexthop specified, as this will drop packets when used as the nexthop.

Use the **no** variant of this command to remove a policy route.

**Syntax** `ip policy-route [<1-500>] [match <application-name>] [from <source-entity>] [to <destination-entity>] nexthop {<interface-list>|<ip-add-list>}`  
`no ip policy-route <1-500>`

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-500>              | The policy route ID number.<br>If you do not specify an ID number, the device assigns the new policy route the next available number, in multiples of 10. For example, if the highest numbered policy route is 81, the next policy route would be given an ID of 90.<br>Policy routes are checked in order of ID number, starting with the lowest ID number. The device applies the policy route as soon as it finds a matching route; it does not check the remaining policy routes. |
| <application-name>   | An application name.<br>You can use the tab key to auto-complete application names.                                                                                                                                                                                                                                                                                                                                                                                                   |
| <source-entity>      | A source entity name.<br>You can use the tab key to auto-complete entity names.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <destination-entity> | A destination entity name.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <interface-list>     | The name of the egress interface or interfaces. You can list up to 8 interfaces per policy route; the device sends the traffic out the first interface in the list that is up.                                                                                                                                                                                                                                                                                                        |
| <ip-add-list>        | The IP address of the next-hop. You can list up to 8 next-hop addresses per policy route; the device sends the traffic to the first address in the list that is reachable. Do not use this when the next-hop is on a dynamic interface (e.g. PPPoE); specify the interface name instead.                                                                                                                                                                                              |

**Default** No policy routes

**Mode** Policy-based Routing Configuration

**Usage notes** You must specify at least one of the **match**, **from** or **to** parameters. Packets will be routed to the specified next-hop if they match the application, come from the source entity, and are destined for the destination entity.

Before creating a policy route, you need to create the application and entities that specify the traffic you want to route. To create an application, use the [application](#) command. To create entities, use the [zone](#), [network \(zone\)](#), and [host \(network\)](#) commands. To see existing applications and entities, use the [show application](#) and [show entity](#) commands.

**Examples** To create a policy route to route traffic that matches an application called 'voice', comes from the entity called 'inside', and is destined for the entity called 'outside', use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ip policy-route 10 match voice from inside
to outside nexthop 10.37.236.65
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ip policy-route 10
```

To route the above traffic via ppp0 if ppp0 is up, or ppp1 if ppp0 is down, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ip policy-route 20 match voice from inside
to outside nexthop ppp0 ppp1
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ip policy-route 20
```

**Related commands**

- [policy-based-routing](#)
- [policy-based-routing enable](#)
- [show application](#)
- [show entity](#)
- [show ip pbr route](#)

**Command changes** Version 5.4.8-0.2: number of routes increased, null interface added

# ip-version (linkmon-probe)

**Overview** Use this command to set the IP version for the Link Health Monitoring ICMP probe. Use the **no** variant of this command to set it back to the default.

**Syntax** `ip-version {4|6}`  
`no ip-version`

| Parameter | Description                        |
|-----------|------------------------------------|
| 4         | Internet Protocol (IPv4)           |
| 6         | Internet Protocol version 6 (IPv6) |

**Default** IPv4

**Mode** Linkmon HTTP Probe Configuration, or Linkmon ICMP Probe Configuration

**Example** To set the IP version as IPv6 for a probe named 'probe1', use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# ip-version 6
```

To set the IP version back to the default for a probe named 'probe1', use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# no ip-version
```

**Command changes** Version 5.4.8-1.1: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches



# ipv6 policy-route

**Overview** Use this command to configure IPv6 policy routes. These routes specify how the device will route traffic from specified applications and entities. You can specify the route's next-hop by specifying the egress interface, or by specifying the next-hop device's IPv6 address (except on dynamic interfaces such as PPPoE). You can also list alternative next-hops to use if your first choice is down.

You can also specify the pseudo interface Null. Null should be the last nexthop specified, as this will drop packets when used as the nexthop.

Use the **no** variant of this command to remove a policy route.

**Syntax** `ipv6 policy-route [<1-500>] [match <application-name>] [from <source-entity>] [to <destination-entity>] nexthop {<interface-list>|<ipv6-add-list>}`  
`no ipv6 policy-route <1-500>`

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-500>              | The policy route ID number.<br>If you do not specify an ID number, the device assigns the new policy route the next available number, in multiples of 10. For example, if the highest numbered policy route is 81, the next policy route would be given an ID of 90.<br>Policy routes are checked in order of ID number, starting with the lowest ID number. The device applies the policy route as soon as it finds a matching route; it does not check the remaining policy routes. |
| <application-name>   | An application name.<br>You can use the tab key to auto-complete application names.                                                                                                                                                                                                                                                                                                                                                                                                   |
| <source-entity>      | A source entity name.<br>You can use the tab key to auto-complete entity names.                                                                                                                                                                                                                                                                                                                                                                                                       |
| <destination-entity> | A destination entity name.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <interface-list>     | The name of the egress interface or interfaces. You can list up to 8 interfaces per policy route; the device sends the traffic out the first interface in the list that is up.                                                                                                                                                                                                                                                                                                        |
| <ipv6-add-list>      | The IPv6 address of the next-hop, specified in the form X:X::X:X. You can list up to 8 next-hop addresses per policy route; the device sends the traffic to the first address in the list that is reachable.<br>Do not use this when the next-hop is on a dynamic interface (e.g. PPPoE); specify the interface name instead.                                                                                                                                                         |

**Default** No policy routes

**Mode** Policy-based Routing Configuration

**Usage notes** You must specify at least one of the **match**, **from** or **to** parameters. Packets will be routed to the specified next-hop if they match the application, come from the source entity, and are destined for the destination entity.

Before creating a policy route, you need to create the application and entities that specify the traffic you want to route. To create an application, use the [application](#) command. To create entities, use the [zone](#), [network \(zone\)](#), and [host \(network\)](#) commands. To see existing applications and entities, use the [show application](#) and [show entity](#) commands.

**Examples** To create a policy route to route traffic that matches an application called 'voice', comes from the entity called 'inside', and is destined for the entity called 'outside', use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ipv6 policy-route 10 match voice from
inside to outside nexthop 2001:100::1
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ipv6 policy-route 10
```

To route the above traffic via ppp0 if ppp0 is up, or ppp1 if ppp0 is down, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# policy-based-routing enable
awplus(config-pbr)# ipv6 policy-route 20 match voice from
inside to outside nexthop ppp0 ppp1
```

To delete the policy route created above, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-based-routing
awplus(config-pbr)# no ipv6 policy-route 20
```

**Related commands**

- [policy-based-routing](#)
- [policy-based-routing enable](#)
- [show application](#)
- [show entity](#)
- [show ipv6 pbr route](#)

**Command changes** Version 5.4.8-0.2: number of routes increased, null interface added

# jitter

**Overview** Use this command to configure the thresholds for the jitter metric. This metric is used to judge whether probes associated with this performance profile are good or bad.

Use the **no** variant of this command to remove jitter bad-above and jitter good-below ranges.

**Syntax** jitter bad-above <unacceptable-jitter-point>  
jitter good-below <acceptable-jitter-point>  
no jitter bad-above  
no jitter good-below

| Parameter                                | Description                                                                                                                                                                                                                                        |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bad-above<br><unacceptable-jitter-point> | The point above which jitter is unacceptable in range <1-1000> in milliseconds.<br>When a probe associated with this profile has a jitter result greater than this value, the associated Link Health Monitoring member will be considered 'bad'.   |
| good-below<br><acceptable-jitter-point>  | The point at or below which jitter is acceptable in range <1-1000> in milliseconds.<br>When a probe associated with this profile has a jitter result less than this value, the associated Link Health Monitoring member will be considered 'good'. |

**Mode** Linkmon Profile Configuration

**Usage notes** If only **bad-above** is configured, then if the probe results indicate a nexthop is above this value, then that nexthop is considered bad. As soon as the results fall below this value, the nexthop will be immediately considered good.

The combination of these two parameters allow for hysteresis, which may prevent link-flapping behavior. For example, with a **bad-above** value of 100, and a **good-below** value of 90, if the jitter rises to 100 the link will be marked 'bad', but it will not be marked 'good' until it reaches or falls below 90.

If only **good-below** is configured, then probe results will not cause a nexthop to be considered bad.

**Example** To configure the point above which jitter is unacceptable to be 100ms and the point at or below which jitter is acceptable to be 90ms for a performance profile named 'profile1', use the following commands:

```
awplus(config)# linkmon profile profile1
awplus(config-linkmon-profile)# jitter bad-above 100
awplus(config-linkmon-profile)# jitter good-below 90
```

To delete the jitter ranges for a performance profile named 'profile1', use the following commands:

```
awplus(config)# linkmon profile profile1
awplus(config-linkmon-profile)# no jitter bad-above
awplus(config-linkmon-profile)# no jitter good-below
```

**Related  
commands**

[ip policy-route](#)  
[latency](#)  
[member \(linkmon-group\)](#)  
[linkmon probe](#)  
[linkmon profile](#)  
[pktloss](#)  
[preference](#)

**Command  
changes**

Version 5.4.8-0.2: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# latency

**Overview** Use this command to configure the thresholds for the latency metric. This metric is used to judge whether probes associated with this performance profile are good or bad.

Use the **no** variant of this command to remove latency bad-above and latency good-below ranges.

**Syntax** `latency bad-above <unacceptable-latency-point>`  
`latency good-below <acceptable-latency-point>`  
`no latency bad-above`  
`no latency good-below`

| Parameter                                                                 | Description                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>bad-above</code><br><code>&lt;unacceptable-latency-point&gt;</code> | The point above which latency is unacceptable in range <code>&lt;1-2000&gt;</code> in milliseconds.<br>When a probe associated with this profile has a latency result greater than this value, the associated Link Health Monitoring member will be considered 'bad'.   |
| <code>good-below</code><br><code>&lt;acceptable-latency-point&gt;</code>  | The point at or below which latency is acceptable in range <code>&lt;1-2000&gt;</code> in milliseconds.<br>When a probe associated with this profile has a latency result less than this value, the associated Link Health Monitoring member will be considered 'good'. |

**Mode** Linkmon Profile Configuration

**Usage notes** If only **bad-above** is configured, then if the probe results indicate a nexthop is above this value, then that nexthop is considered bad. As soon as the results fall below this value, the nexthop will be immediately considered good.

The combination of these two parameters allow for hysteresis, which may prevent link-flapping behavior. For example, with a **bad-above** value of 100, and a **good-below** value of 90, if the latency rises to 100 the link will be marked 'bad', but it will not be marked 'good' until it reaches or falls below 90.

If only **good-below** is configured, then probe results will not cause a nexthop to be considered bad.

**Example** To configure the point above which latency is unacceptable to be 100ms and the point at or below which latency is acceptable to be 90ms for a performance profile named 'profile1', use the following commands:

```
awplus(config)# linkmon profile profile1
awplus(config-linkmon-profile)# latency bad-above 100
awplus(config-linkmon-profile)# latency good-below 90
```

To delete the latency ranges for a performance profile named 'profile1', use the following commands:

```
awplus(config)# linkmon profile profile1
awplus(config-linkmon-profile)# no latency bad-above
awplus(config-linkmon-profile)# no latency good-below
```

**Related  
commands**

[ip policy-route](#)  
[jitter](#)  
[member \(linkmon-group\)](#)  
[linkmon probe](#)  
[linkmon profile](#)  
[pktloss](#)  
[preference](#)

**Command  
changes**

Version 5.4.8-0.2: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# linkmon group

**Overview** Use this command to create a Link Health Monitoring group and enter Linkmon Group Configuration mode where this group can be configured.

Use the **no** variant of this command to remove a configured group. All members previously belonging to the group are also removed.

**Syntax** `linkmon group <group-name>`  
`no linkmon group <group-name>`

| Parameter                       | Description                            |
|---------------------------------|----------------------------------------|
| <code>&lt;group-name&gt;</code> | The name of the link monitoring group. |

**Mode** Global Configuration

**Example** To create a new link monitoring group named 'group1', use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon group group1
awplus(config-linkmon-group)#
```

To remove a link monitoring group named 'group1', use the following commands:

```
awplus# configure terminal
awplus(config)# no linkmon group group1
```

**Related commands**

- [ip policy-route](#)
- [jitter](#)
- [latency](#)
- [linkmon probe](#)
- [linkmon profile](#)
- [load-balancing](#)
- [member \(linkmon-group\)](#)
- [pktloss](#)
- [preference](#)
- [show linkmon probe](#)

**Command changes** Version 5.4.8-1.1: command added

# linkmon probe-history

**Overview** Use this command to create a collection instance that records the metrics gathered by a Link Health Monitoring probe.

Use the **no** variant of this command to remove the specified collection instance.

**Syntax** `linkmon probe-history [<1-65535>] probe <probe-name> interval <1-2678400> buckets <1-65535>`  
`no linkmon probe-history <1-65535>`

| Parameter                  | Description                                                                                                              |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------|
| probe-history<br><1-65535> | The ID of the probe history collection instance. If this is not set on creation then it will be automatically allocated. |
| probe<br><probe-name>      | The name of the probe to record metrics for.                                                                             |
| interval<br><1-2678400>    | The interval that metrics are collated, in seconds.                                                                      |
| buckets<br><1-65535>       | The maximum number of metric history samples.                                                                            |

**Mode** Global Configuration

**Usage notes** Metrics are collated every **interval** seconds. Up to **buckets** samples of metrics are collated.

Different **interval** and **buckets** values can be used to record specific kinds of histories. For example, an **interval** value of 1 and a **buckets** value of 3600 would record per second metrics of a probe for an hour. An **interval** value of 3600 and a **buckets** value of 744 would record per hour metrics of a probe for 31 days.

Using the Web API, metric values for a sample are returned as a sum and a count. The sum can be divided by the count for an average. For example, if 10 probes have been sent during a history interval, then the metric counts would be 10 for a sample, and the sum would be the total of the metric values.

If a probe receives no reply then no metric is recorded.

Packet loss is not recorded exactly. Instead the probes sent and probe replies received is recorded.

**CAUTION:** This configuration option can consume a large amount of RAM on the device, particularly if you configure high numbers of buckets. The memory is reserved when the command is entered, so if the memory consumption from this command is too high, entering the command will trigger the device's low memory management procedure. The device will continue to operate when it reaches a low memory state, but if available memory decreases further into a critical zone, a warning message will be printed and the device will reboot.



**Example** To create a Link Health Monitoring probe history collection instance with an ID of 10 for a probe named 'probe1' that collates metrics every second while keeping up to 300 samples, use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon probe-history 10 probe probe1 interval
1 buckets 300
```

To create a Link Health Monitoring probe history collection instance with an automatically allocated ID for a probe named 'probe1' that collates metrics every 60 seconds while keeping up to 3600 samples, use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon probe-history probe probe1 interval 60
buckets 3600
```

**Related commands** [linkmon probe](#)

**Command changes** Version 5.4.8-0.2: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# linkmon probe

**Overview** Use this command to create a Link Health Monitoring probe and enter the appropriate Link Health Monitoring Probe Configuration Mode where this probe can be configured.

Use the **no** variant of this command to delete the Link Health Monitoring probe.

**Syntax** `linkmon probe name <probe-name> [type {icmp-ping|http-get}]`  
`no linkmon probe name <probe-name>`

| Parameter    | Description                                                                                                                                                                                                                    |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <probe-name> | The name of the probe.                                                                                                                                                                                                         |
| type         | The type of the probe. Indicates the packet type or protocol used by the probe, either of icmp-ping (ICMP) or http-get (HTTP). This parameter is optional. If not entered, a newly created probe's type defaults to icmp-ping. |

**Default** The default probe type for a newly created probe is **icmp-ping**. The optional parameter **type** is only required to create a probe type other than the default. The **type** parameter is not required when editing an existing probe or deleting a probe.

**Mode** Global Configuration

**Usage notes** The optional probe **type** parameter represents the packet type or protocol used in the transmission of the probe. A probe of type **icmp-ping** will present some different configuration options to a probe of type **http-get**.

An **icmp-ping** Link Health Monitoring probe requires a destination, and must be enabled for probing to begin.

An **http-get** Link Health Monitoring probe requires a URL, and must be enabled for probing to begin.

**Example** To create a probe named 'probe1' using the default probe type and enter Link Health Monitoring ICMP Probe Configuration Mode to configure it, use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)#
```

To create a probe named 'probe1' using the default ICMP probe type and enter Link Health Monitoring ICMP Probe Configuration Mode to configure it, use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon probe name probe1 type icmp-ping
awplus(config-linkmon-icmp-probe)#
```

To create a probe named 'probe1' using the HTTP probe type and enter Link Health Monitoring HTTP Probe Configuration Mode to configure it, use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon probe name probe1 http-probe
awplus(config-linkmon-http-probe)#
```

To remove a probe named 'probe1', use the following commands:

```
awplus# configure terminal
awplus(config)# no linkmon probe name probe1
```

**Related  
commands**

[enable \(linkmon-probe\)](#)  
[interval \(linkmon-probe\)](#)  
[ip policy-route](#)  
[jitter](#)  
[latency](#)  
[linkmon probe-history](#)  
[linkmon profile](#)  
[member \(linkmon-group\)](#)  
[pktloss](#)  
[preference](#)  
[show linkmon probe](#)  
[show linkmon probe-history](#)  
[size \(linkmon-probe\)](#)

**Command  
changes**

Version 5.4.8-0.2: command added

Version 5.4.8-1.1: now operates as a modal command, with the new type parameter used to determine whether to enter ICMP or HTTP probe mode

Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# linkmon profile

**Overview** Use this command to create a Link Health Monitoring performance profile and enter Linkmon Profile Configuration mode where this profile can be configured.

Use the **no** variant of this command to remove a configured performance profile.

**Syntax** `linkmon profile <profile-name>`  
`no linkmon profile <profile-name>`

| Parameter                         | Description                          |
|-----------------------------------|--------------------------------------|
| <code>&lt;profile-name&gt;</code> | The name of the performance profile. |

**Mode** Global Configuration

**Example** To create a new performance profile named 'profile1', use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon profile profile1
awplus(config-linkmon-profile)#
```

To remove a performance profile named 'profile1', use the following commands:

```
awplus# configure terminal
awplus(config)# no linkmon profile profile1
```

**Related commands**

- [ip policy-route](#)
- [jitter](#)
- [latency](#)
- [linkmon probe](#)
- [member \(linkmon-group\)](#)
- [pktloss](#)
- [preference](#)
- [show linkmon probe](#)

**Command changes**

- Version 5.4.8-0.2: command added
- Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# load-balancing

**Overview** Use this command to enable load-balancing for a Link Health Monitoring group.  
Use the **no** variant of this command to remove load-balancing from a Link Health Monitoring group.

**Syntax** `load-balancing`  
`no load-balancing`

**Default** Load-balancing is disabled.

**Mode** Linkmon Group Configuration

**Usage notes** When load-balancing is enabled, traffic will be load-balanced across all valid nexthops.

Load-balancing is achieved using a hashing algorithm on a per-flow basis for each application. For example, if two users visit YouTube, the session for user 1 may be sent over Tunnel 1, and the session for user 2 may be sent over Tunnel 2. Packets from each session will be sent entirely within one tunnel, until that session ends.

When a Link Health Monitoring group is configured for load-balancing, the preferred-metric used in any profile that is combined with the group in a PBR rule will be ignored when selecting 'good' links to send traffic over. This is because when load-balancing is enabled, all links that are 'good' are selected to send traffic over, so preferred metric is not required for tie-breaking. The preferred-metric is still used when all links within a group are considered 'bad' by a profile, in which case the least-bad link according to the preferred metric will be selected as the single link to send traffic over.

**Example** To enable load-balancing on the Link Health Monitoring group "BranchOffice", use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon group BranchOffice
awplus(config-linkmon-group)# load-balancing
```

To disable load-balancing on the Link Health Monitoring group "BranchOffice", use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon group BranchOffice
awplus(config-linkmon-group)# no load-balancing
```

**Related commands** [linkmon group](#)

**Command changes** Version 5.4.8-1.1: command added

# member (linkmon-group)

**Overview** Use this command to create a link monitoring group member and specify its nexthop destination and the probe to be used to gather metrics to judge the health of this member. A maximum of 8 members can be created per group.

Use the **no** variant of this command to remove a group member. The member ID is mandatory upon deletion.

**Syntax** member [*<member-id>*] destination *<ip-address>*|*<interface>* probe *<probe-name>*  
no member *<member-id>*

| Parameter                 | Description                                                                                                                                                                                        |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;member-id&gt;</i>  | The ID of the link monitoring group member, a number in range <i>&lt;1-128&gt;</i> .                                                                                                               |
| destination               | The nexthop destination of the member that traffic will be directed to when this member is judged as the best available within the group, according the probe metric results and PBR rule profile. |
| <i>&lt;ip-address&gt;</i> | The IPv4 or IPv6 IP address of the next-hop. Do not use this when the next-hop is on a dynamic interface (e.g. PPPoE); specify the interface name instead.                                         |
| <i>&lt;interface&gt;</i>  | The name of the egress interface of the next-hop.                                                                                                                                                  |
| <i>&lt;probe-name&gt;</i> | The name of an existing probe.                                                                                                                                                                     |

**Mode** Linkmon Group Configuration

**Usage notes** Users can also optionally specify a group member ID. If no ID is specified, a unique ID will be automatically created and assigned to the group member.

The pseudo interface Null can be specified as a nexthop. This acts as an always up but bad interface. This is to be chosen as the best member when all other members are unavailable. No probe needs to be specified for this type of member.

**Example** To create a new group member in group 'group1' using probe 'probe1' with ID 10 and destination 'tunnel1', use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon group group1
awplus(config-linkmon-group)# member 10 destination tunnel1
probe probe1
```

To delete the group member with member ID '10' in group 'group1', use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon group group1
awplus(config-linkmon-group)# no member 10
```

**Related  
commands**

[ip policy-route](#)  
[member \(linkmon-group\)](#)  
[linkmon profile](#)  
[linkmon probe](#)  
[show linkmon probe](#)

**Command  
changes**

Version 5.4.8-0.2: command added

# pktloss

**Overview** Use this command to configure the thresholds for the packet loss metric. This metric is used to judge whether probes associated with this performance profile are good or bad.

Use the **no** variant of this command to remove packet loss rate bad-above and packet loss rate good-below ranges.

**Syntax** `pktloss bad-above <unacceptable-pktloss-point>`  
`pktloss good-below <acceptable-pktloss-point>`  
`no pktloss bad-above`  
`no pktloss good-below`

| Parameter                                       | Description                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;unacceptable-pktloss-point&gt;</code> | The point above which packet loss rate is unacceptable in range <code>&lt;0.0-100.0&gt;</code> in percent to one decimal place. When a probe associated with this profile has a packet loss rate result greater than this value, the associated Link Health Monitoring member will be considered 'bad'.   |
| <code>&lt;acceptable-pktloss-point&gt;</code>   | The point at or below which packet loss rate is acceptable in range <code>&lt;0.0-100.0&gt;</code> in percent to one decimal place. When a probe associated with this profile has a packet loss rate result less than this value, the associated Link Health Monitoring member will be considered 'good'. |

**Mode** Linkmon Profile Configuration

**Usage notes** If only **bad-above** is configured, then if the probe results indicate a nexthop is above this value, then that nexthop is considered bad. As soon as the results fall below this value, the nexthop will be immediately considered good.

The combination of these two parameters allow for hysteresis, which may prevent link-flapping behavior. For example, with a **bad-above** value of 5, and a **good-below** value of 3, if the packet loss rises to 5 the link will be marked 'bad', but it will not be marked 'good' until it reaches or falls below 3.

If only **good-below** is configured, then probe results will not cause a nexthop to be considered bad.

Packet loss also has a built-in threshold, where when it reaches 100% packet loss, the associated member is automatically considered unreachable / down, and will never be used as a nexthop for packets that match the PBR rule. If all members within a group are unreachable in this manner, then traffic will be routed via default routing behavior, rather than PBR. If the group has a member configured with a NULL destination, when all other members in the group are unreachable, traffic will be dropped (blackhole routed) instead.



**Example** To configure the point above which packet loss rate is unacceptable to be 5% and the point at or below which packet loss rate is acceptable to be 3.0% for a performance profile named 'profile1', use the following commands:

```
awplus(config)# linkmon profile profile1
awplus(config-linkmon-profile)# pktloss bad-above 5.0
awplus(config-linkmon-profile)# pktloss good-below 3.0
```

To delete the packet loss rate ranges for a performance profile named 'profile1', use the following commands:

```
awplus(config)# linkmon profile profile1
awplus(config-linkmon-profile)# no pktloss bad-above
awplus(config-linkmon-profile)# no pktloss good-below
```

**Related commands**

[ip policy-route](#)  
[jitter](#)  
[latency](#)  
[member \(linkmon-group\)](#)  
[linkmon probe](#)  
[linkmon profile](#)  
[preference](#)

**Command changes** Version 5.4.8-0.2: command added

# preference

**Overview** Use this command to configure the preferred metric of probes that use this Link Health Monitoring performance profile.

Use the **no** variant of this command to remove a preference.

**Syntax** `preference {latency|jitter|pktloss}`  
`no preference`

| Parameter | Description                                     |
|-----------|-------------------------------------------------|
| latency   | Use latency as the tie-breaker metric.          |
| jitter    | Use jitter as the tie-breaker metric.           |
| pktloss   | Use packet loss rate as the tie-breaker metric. |

**Default** No preference is applied.

**Mode** Linkmon Profile Configuration

**Usage notes** When two or more members within the same group have the same link-health judgment (good, bad), the metric nominated as the preferred one is used as a tie-break to select the best member amongst those that are tied. If the metric values for the preferred metric are identical, or preferred metric is not set in the profile, then the member with the lowest ID is selected as the best one.

**Example** To choose maximum allowable latency to be the preferred metric for a performance profile named 'profile1', use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon profile profile1
awplus(config-linkmon-profile)# preference latency
```

To delete an existing preference for a performance profile named 'profile1', use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon profile profile1
awplus(config-linkmon-profile)# no preference
```

**Related commands**

- [ip policy-route](#)
- [jitter](#)
- [latency](#)
- [member \(linkmon-group\)](#)
- [linkmon probe](#)
- [linkmon profile](#)

pktloss

**Command changes**    Version 5.4.8-0.2: command added

# sample-size (linkmon-probe)

**Overview** Use this command to set the sample size used for calculating latency and jitter metrics for a Link Health Monitoring probe.

Use the **no** variant of this command to set the sample size back to the default value.

**Syntax** `sample-size <1-100>`  
`no sample-size`

| Parameter                  | Description                                                                         |
|----------------------------|-------------------------------------------------------------------------------------|
| <code>&lt;1-100&gt;</code> | The number of probe samples to use when calculating the latency and jitter metrics. |

**Default** The default sample size is 5.

**Mode** Linkmon ICMP Probe Configuration

**Example** To set the sample size a probe named 'probe1' to 10, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# sample-size 10
```

To set the sample size a probe named 'probe1' back to the default, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# no sample-size
```

**Related commands** [linkmon probe](#)

**Command changes** Version 5.4.8-1.1: command added

Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# show debugging linkmon

**Overview** Use this command to display the output of link monitoring debugging settings.

**Syntax** show debugging linkmon

**Mode** Privileged Exec

**Example** To show the current debugging settings for link monitoring, use the following command:

```
awplus# show debugging linkmon
```

**Output** Figure 27-1: Example output from **show debugging linkmon**

```
awplus#show debugging linkmon
 probes TUNNEL10
 TUNNEL20
 groups GROUP1
 GROUP2
 ip address debugging is off
 interface debugging is on
 pbr-group debugging is on
```

Table 27-1: Parameters in the output from **show debugging linkmon**

| Parameter            | Description                                                         |
|----------------------|---------------------------------------------------------------------|
| probes               | A list of the Link Health Monitoring probes with debugging enabled. |
| groups               | A list of the Link Health Monitoring groups with debugging enabled. |
| ip address debugging | Whether IP address debugging is enabled.                            |
| interface debugging  | Whether interface debugging is enabled.                             |
| pbr-group debugging  | Whether PBR-group debugging is enabled.                             |

**Related commands** [debug linkmon](#)

**Command changes** Version 5.4.8-0.2: command added

# show linkmon probe

**Overview** Use this command to display output for one or all link monitoring probes.

**Syntax** show linkmon probe [<probe-name>]

| Parameter    | Description                                |
|--------------|--------------------------------------------|
| <probe-name> | The name of the specific probe to display. |

**Mode** User Exec and Privileged Exec

**Example** To show the output for all link monitoring probes, use the following command:

```
awplus# show linkmon probe
```

To show the output for a link monitoring probe named 'probe1', use the following command:

```
awplus# show linkmon probe probe1
```

**Output** Figure 27-2: Example output from **show linkmon probe**

```
BRANCH#show linkmon probe
Probe Name : Head-Office-VPN1
Status : enabled
Type : ICMP
IP version : IPv4
Destination : 198.51.100.1
Egress Int : -
Source : -
DSCP : -
Packet Size : -
Interval : -
Sample Size : -
Latest Metrics
 Latency : 1001ms
 Jitter : 0ms
 Packet Loss : 0.0%
Probe Details
 Probes Sent : 3154
 Last Probe Sent : 23 Mar 2018 03:36:00
 Last Probe Received : 23 Mar 2018 03:36:00

Probe Name : Head-Office-VPN2
Status : enabled
Type : ICMP
```

|                     |                        |
|---------------------|------------------------|
| IP version          | : IPv4                 |
| Destination         | : 203.0.113.1          |
| Egress Int          | : -                    |
| Source              | : -                    |
| DSCP                | : -                    |
| Packet Size         | : -                    |
| Interval            | : -                    |
| Sample Size         | : -                    |
| Latest Metrics      |                        |
| Latency             | : 1000ms               |
| Jitter              | : 0ms                  |
| Packet Loss         | : 0.0%                 |
| Probe Details       |                        |
| Probes Sent         | : 3154                 |
| Last Probe Sent     | : 23 Mar 2018 03:36:00 |
| Last Probe Received | : 23 Mar 2018 03:36:00 |

Table 27-2: Parameters in the output from **show linkmon probe**

| Parameter        | Description                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name             | The name of the probe.                                                                                                                                                     |
| Status           | Whether the probe is enabled or disabled. If it is enabled, then the device will attempt to send probes if the link is up. If it is disabled, then no probes will be sent. |
| Type             | The type of probe packet sent.                                                                                                                                             |
| IP version       | The IP version being used, IPv4 or IPv6.                                                                                                                                   |
| Destination      | The destination IP address that the probes are sent to.                                                                                                                    |
| Egress Interface | The interface that the probe packets should egress.                                                                                                                        |
| Source           | The source IP address or interface.                                                                                                                                        |
| DSCP             | The DSCP value to use when sending the packet.                                                                                                                             |
| Packet Size      | The size of a probe packet.                                                                                                                                                |
| Interval         | The number of milliseconds between sending out each probe.                                                                                                                 |
| Sample Size      | The number of probe results to use when calculating the latency and jitter metrics.                                                                                        |
| Latency          | The average latency based on the last <b>sample size</b> samples.                                                                                                          |
| Jitter           | The average jitter based on the last <b>sample size</b> samples.                                                                                                           |
| Packet Loss      | The percentage of packets lost based on the last 100 probes.                                                                                                               |

Table 27-2: Parameters in the output from **show linkmon probe** (cont.)

| Parameter           | Description                                                         |
|---------------------|---------------------------------------------------------------------|
| Probes Sent         | The number of probe packets that have been sent.                    |
| Last Probe Sent     | The time that the last probe packet was sent.                       |
| Last Probe Received | The time that the device last successfully received a probe packet. |

**Related commands** [linkmon probe](#)

**Command changes** Version 5.4.8-0.2: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches



# show linkmon probe-history

**Overview** Use this command to show information about Link Health Monitoring probe metric history collection instances.

**Syntax** `show linkmon probe-history [<1-65535>|probe <probe-name>]`

| Parameter    | Description                                            |
|--------------|--------------------------------------------------------|
| <1-65535>    | The ID of the collection instance to show history for. |
| <probe-name> | The name of the probe to show history for.             |

**Mode** User Exec and Privileged Exec

**Example** To show all Link Health Monitoring probe history collection instances, use the following command:

```
awplus# show linkmon probe-history
```

To show a Link Health Monitoring probe history collection instance with the ID of '10', use the following command:

```
awplus# show linkmon probe-history 10
```

To show all Link Health Monitoring probe history collection instances that are using a probe named 'probe1', use the following command:

```
awplus# show linkmon probe-history probe probe1
```

**Output** Figure 27-3: Example output from **show linkmon probe-history**

|                                   |              |         |                   |       |          |  |
|-----------------------------------|--------------|---------|-------------------|-------|----------|--|
| awplus#show linkmon probe-history |              |         |                   |       |          |  |
| -----                             |              |         |                   |       |          |  |
| ID                                | Interval (s) | Buckets | Latency (ms): Min | Max   | Avg      |  |
| Probe                             |              |         | Jitter (ms): Min  | Max   | Avg      |  |
|                                   |              |         | Packets: Tx       | Rx    | Loss (%) |  |
| -----                             |              |         |                   |       |          |  |
| 10                                | 1            | 300/300 | 94                | 105   | 99       |  |
| PROBE1                            |              |         | 2                 | 11    | 6        |  |
|                                   |              |         | 2978              | 2978  | 0.00     |  |
| 20                                | 5            | 300/300 | 97                | 102   | 99       |  |
| PROBE1                            |              |         | 4                 | 9     | 6        |  |
|                                   |              |         | 14892             | 14892 | 0.00     |  |
| 30                                | 10           | 300/300 | 98                | 101   | 100      |  |
| PROBE1                            |              |         | 5                 | 8     | 6        |  |
|                                   |              |         | 29785             | 29785 | 0.00     |  |

Table 27-3: Parameters in the output from **show linkmon probe-history**

| Parameter    | Description                                                  |
|--------------|--------------------------------------------------------------|
| ID           | The ID of the Link Health Monitoring probe-history.          |
| Probe        | The name of the probe that this history is for.              |
| Interval     | The amount of time between each history sample (in seconds). |
| Buckets      | The total number of samples that are stored.                 |
| Latency min  | The minimum latency that is in the history.                  |
| Latency max  | The maximum latency that is in the history.                  |
| Latency avg  | The average latency of the samples stored in the history.    |
| Jitter min   | The minimum jitter that is in the history.                   |
| Jitter max   | The maximum jitter that is in the history.                   |
| Jitter avg   | The average jitter of the samples stored in the history.     |
| Packets Tx   | The total number of packets transmitted in this history.     |
| Packets Rx   | The total number of packets received in this history.        |
| Packets Loss | The percentage of packets lost in the history.               |

**Related commands** [linkmon probe](#)  
[linkmon probe-history](#)

**Command changes** Version 5.4.8-0.2: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# show pbr rules

**Overview** Use this command to display the configured IPv4 and IPv6 policy routes. It also shows the validity of the policy routes.

**Syntax**

```
show pbr rules
show pbr rules <rule-id>
show pbr rules profile <profile-name>
show pbr rules group <group-name>
```

| Parameter      | Description                                                                                                                                                                                  |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <rule-id>      | The policy route ID. If you specify a policy route ID, the output only lists configuration and status for this specified rule.                                                               |
| <profile-name> | The Link Health Monitoring profile name. If you specify an existing Link Health Monitoring performance profile name, the output only lists profile configuration for this specified profile. |
| <group-name>   | The Link Health Monitoring group name. If you specify an existing Link Health Monitoring group name, the output only lists group configuration for this specified profile.                   |

**Mode** User Exec and Privileged Exec

**Example** To show information about the policy routes, use the following command:

```
awplus# show pbr rules
```

To show information about the policy route rule with the rule ID of '1', use the following command:

```
awplus# show pbr rules 1
```

To show information about the Link Health Monitoring profile with the profile name of 'profile1', use the following command:

```
awplus# show pbr rules profile profile1
```

To show information about the Link Health Monitoring group with the profile name of 'group1', use the following command:

```
awplus# show pbr rules group group1
```

**Output** Figure 27-4: Example output from **show pbr rules**

```
awplus#show pbr rules
Statistics:

Route table usage: 1/500
Total number of configured PBR-rules = 1

PBR-Rule 1

Active: Yes
Match: sip
From: LAN
To: any
Profile: PROFILE1
 latency bad above: 300 ms
 latency good below: - ms
 jitter bad above: - ms
 jitter good below: - ms
 pktloss bad above: - %
 pktloss good below: - %
Group: GROUP1
 Member: 10
 next-hop: 172.16.10.1
 probe: PROBE10
 latency: 401 ms
 jitter: 0 ms
 pktloss: 0.0 %
 Member: 20
 next-hop: 172.16.20.1
 probe: PROBE20
 latency: 400 ms
 jitter: 0 ms
 pktloss: 0.0 %
Last Change:
 Current Nexthop: 172.16.10.1
 Previous Nexthop: -
 Change Time: 22 Nov 2017 13:57:48
 Causes: Rx probe 'PROBE10', latency (401>300) ms
 Decision: only available link
 Change Count: 1
```

Figure 27-5: Example output from **show pbr rules 1**

```
awplus#show pbr rules 1
PBR-Rule 1

Active: Yes
Match: sip
From: LAN
To: any
Profile: PROFILE1
 latency bad above: 300 ms
 latency good below: - ms
 jitter bad above: - ms
 jitter good below: - ms
 pktloss bad above: - %
 pktloss good below: - %
Group: GROUP1
 Member: 10
 next-hop: 172.16.10.1
 probe: PROBE10
 latency: 401 ms
 jitter: 0 ms
 pktloss: 0.0 %
 Member: 20
 next-hop: 172.16.20.1
 probe: PROBE20
 latency: 400 ms
 jitter: 0 ms
 pktloss: 0.0 %
Last Change:
 Current Nexthop: 172.16.10.1
 Previous Nexthop: -
 Change Time: 22 Nov 2017 13:57:48
 Causes: Rx probe 'PROBE10', latency (401>300) ms
 Decision: only available link
Change Count: 1
```

Figure 27-6: Example output from **show pbr rules profile profile1**

```
awplus#show pbr rules profile profile1
Profile: profile1
 latency bad above: 300 ms
 latency good below: - ms
 jitter bad above: - ms
 jitter good below: - ms
 pktloss bad above: - %
 pktloss good below: - %
```

Figure 27-7: Example output from **show pbr rules group group1**

```
awplus#show pbr rules group group1
Group: group1
 Member: 10
 next-hop: 172.16.10.1
 probe: PROBE10
 latency: 401 ms
 jitter: 0 ms
 pktloss: 0.0 %
 Member: 20
 next-hop: 172.16.20.1
 probe: PROBE20
 latency: 400 ms
 jitter: 0 ms
 pktloss: 0.0 %
```

Table 27-4: Parameters in the output from **show pbr rules**

| Parameter                            | Description                                                                                                                                                                                    |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Total number of configured PBR-rules | The number of PBR rules currently configured. This includes both conventional PBR policy-routes and Link Health Monitoring IP policy-routes, regardless of whether the rules are valid or not. |
| PBR-Rule                             | The PBR rule ID which the following statistics and configuration are associated with.                                                                                                          |
| Active                               | Whether the rule is active or not.                                                                                                                                                             |
| Match                                | The name of an application. Packets will be routed to the specified next hop if they match this application, come from the source entity, and are destined for the destination entity.         |
| From                                 | The name of the source entity. Packets will be routed to the specified next hop if they match the application, come from this source entity, and are destined for the destination entity.      |
| To                                   | The name of the destination entity. Packets will be routed to the specified next hop if they match the application, come from the source entity, and are destined for this destination entity. |
| Profile                              | The name of the Link Health Monitoring profile associated with this Link Health Monitoring PBR policy-route.                                                                                   |
| bad above,<br>good below             | The configured threshold for this specific rule. There are fields for latency, jitter, and packet loss. If this field has a value of "-", then the threshold has not been configured.          |
| Group                                | The name of the Link Health Monitoring group associated with this Link Health Monitoring PBR policy-route.                                                                                     |

Table 27-4: Parameters in the output from **show pbr rules** (cont.)

| Parameter        | Description                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Member           | The ID of the Link Health Monitoring member associated with this Link Health Monitoring group.                                                        |
| Nexthop          | The IPv4 or IPv6 address of the next-hop or the egress interface. There can be up to 8 next-hops per policy route.                                    |
| probe            | The Link Health Monitoring probe associated with the Link Health Monitoring group member.                                                             |
| latency          | The latency of the probe associated with the Link Health Monitoring member.                                                                           |
| jitter           | The jitter of the probe associated with the Link Health Monitoring member.                                                                            |
| packet loss      | The packet loss of the probe associated with the Link Health Monitoring member.                                                                       |
| Current Nexthop  | The chosen nexthop for traffic matching the Link Health Monitoring PBR policy-route.                                                                  |
| Previous Nexthop | The previously chosen nexthop prior to failover. If a failover hasn't occurred on this setup, there is no previous nexthop. This is indicated by "-". |
| Change Time      | The time at which the current nexthop was chosen. This will change if a failover occurs, or at boot.                                                  |
| Causes           | The event that caused the last failover.                                                                                                              |
| Decision         | The reason why the current nexthop was chosen.                                                                                                        |
| Change Count     | The number of times the chosen nexthop has changed. This counter will increment any time a link failover occurs.                                      |

**Related commands**

[ip policy-route](#)  
[ipv6 policy-route](#)  
[policy-based-routing](#)  
[show ip pbr route](#)  
[show ipv6 pbr route](#)

**Command changes**

Version 5.4.8-0.2: new parameters for profiles and groups added  
Version 5.4.8-1.1: up to 500 route table entries supported

## show pbr rules brief

**Overview** Use this command to show a summary of all PBR rules. It also indicates, by the presence or absence of the nexthop field, which nexthop to route to.

**Syntax** show pbr rules brief

**Mode** User Exec and Privileged Exec

**Example** To show information about the policy routes, use the following command:

```
awplus# show pbr rules brief
```

**Output** Figure 27-8: Example output from **show pbr rules brief**

```
awplus#show pbr rules brief
Policy based routing is enabled
Route table usage: 2/500
* - No route table available for the rule - see "show ip pbr
route"
Rule Match From To Valid Nexthop

10 any entities.any entities.outside Yes 10.10.20.2
20 udp any any Yes 2001:100::2
```

Table 27-5: Parameters in the output from **show pbr rules brief**

| Parameter | Description                                                                                                                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule      | The policy route ID number.<br>Policy routes are checked in order of ID number, starting with the lowest ID number. The device applies the policy route as soon as it finds a matching route; it does not check the remaining policy routes. |
| Match     | The name of an application.<br>Packets will be routed to the specified next hop if they match this application, come from the source entity, and are destined for the destination entity.                                                    |
| From      | The name of the source entity.<br>Packets will be routed to the specified next hop if they match the application, come from this source entity, and are destined for the destination entity.                                                 |
| To        | The name of the destination entity.<br>Packets will be routed to the specified next hop if they match the application, come from the source entity, and are destined for this destination entity.                                            |



Table 27-5: Parameters in the output from **show pbr rules brief** (cont.)

| Parameter | Description                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------|
| Valid     | Whether the application and entities are valid.                                                                    |
| Nexthop   | The IPv4 or IPv6 address of the next-hop or the egress interface. There can be up to 8 next-hops per policy route. |

**Related commands** [show pbr rules](#)

**Command changes** Version 5.4.8-0.2: command added  
Version 5.4.8-1.1: up to 500 route table entries supported

## size (linkmon-probe)

**Overview** Use this command to set the size of the packets used by a Link Health Monitoring probe.

Use the **no** variant of this command to set the size back to the default.

**Syntax** `size <64-1500>`  
`no size`

| Parameter                    | Description                            |
|------------------------------|----------------------------------------|
| <code>&lt;64-1500&gt;</code> | The size of the probe packet in bytes. |

**Default** The default packet size is 100 bytes.

**Mode** Linkmon ICMP Probe Configuration

**Example** To set the size of a probe named 'probe1' to 1000, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# size 1000
```

To set the size of a probe named 'probe1' back to the default, use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# no size
```

**Related commands** [linkmon probe](#)

**Command changes** Version 5.4.8-1.1: command added

Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# source (linkmon-probe)

**Overview** Use this command to set the source IP address or interface for a Link Health Monitoring probe.

Use the **no** variant of this command to return it to the default.

**Syntax** `source {<interface>|<ip-address>}`  
`no source`

| Parameter                       | Description                                                                                                                                                                                         |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;interface&gt;</code>  | The name of the interface that probes are sourcing from. The specified interface needs to be locally configured with at least one valid IPv4 address, and the interface is in up and running state. |
| <code>&lt;ip-address&gt;</code> | The source IPv4 address for this probe. The specified IP address needs to be locally configured on an interface that is in an up-and-running state.                                                 |

**Default** No source IP address is defined by default. The source IP address will be selected using standard routing behavior to reach the probe's destination.

**Mode** Linkmon ICMP Probe Configuration

**Example** To set the source interface as 'lo' for a probe named 'probe1', use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# source lo
```

To set the source interface back to default for a probe named 'probe1', use the following commands:

```
awplus(config)# linkmon probe name probe1
awplus(config-linkmon-icmp-probe)# no source
```

**Related commands** [linkmon probe](#)

**Command changes** Version 5.4.8-1.1: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# url (linkmon-probe)

**Overview** Use this command to set the destination URL of a Link Health Monitoring probe. This is a required configuration option for http-get probes.

Use the **no** variant of this command to remove the URL.

**Syntax** url <url>  
no url

| Parameter | Description                                                                                                                                                                                                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <url>     | The destination the probe is being sent to. The URL must use ASCII characters and conform to the URL syntax in RFC 3986, with http or https protocol at the start and an optional port number on the end, such as :80, :443 or :8080. |

**Mode** Linkmon HTTP Probe Configuration

**Example** To set the destination URL of a Link Health Monitoring probe named “test-probe”, use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon probe name test-probe type http
awplus(config-linkmon-http-probe)# url
http://www.alliedtelesis.co.nz/
```

Some other examples of supported URL formats:

```
awplus(config-linkmon-http-probe)# url
https://www.facebook.com/

awplus(config-linkmon-http-probe)# url
http://intranet.atlnz.lc:8080
```

To remove the URL, use the following commands:

```
awplus# configure terminal
awplus(config)# linkmon probe name test-probe type http
awplus(config-linkmon-http-probe)# no url
```

**Related commands** [linkmon probe](#)

**Command changes** Version 5.4.8-1.1: command added  
Version 5.5.1-0.1: command added to all AlliedWare Plus switches

# Part 4: Multicast Applications

# 28

# IGMP Commands

## Introduction

**Overview** Devices running AlliedWare Plus use IGMP (Internet Group Management Protocol) and MLD (Multicast Listener Discovery) to track which multicast groups their clients belong to. This enables them to send the correct multimedia streams to the correct destinations. IGMP is used for IPv4 multicasting, and MLD is used for IPv6 multicasting.

This chapter describes the commands to configure IGMP Querier behaviour and selection, IGMP Snooping and IGMP Proxy.

- Command List**
- [“clear ip igmp”](#) on page 1332
  - [“clear ip igmp group”](#) on page 1333
  - [“clear ip igmp interface”](#) on page 1334
  - [“debug igmp”](#) on page 1335
  - [“ip igmp”](#) on page 1336
  - [“ip igmp last-member-query-count”](#) on page 1337
  - [“ip igmp last-member-query-interval”](#) on page 1338
  - [“ip igmp mroute-proxy”](#) on page 1339
  - [“ip igmp proxy-service”](#) on page 1340
  - [“ip igmp querier-timeout”](#) on page 1341
  - [“ip igmp query-holdtime”](#) on page 1342
  - [“ip igmp query-interval”](#) on page 1344
  - [“ip igmp query-max-response-time”](#) on page 1346
  - [“ip igmp ra-option”](#) on page 1348
  - [“ip igmp robustness-variable”](#) on page 1349
  - [“ip igmp source-address-check”](#) on page 1350

- [“ip igmp startup-query-count”](#) on page 1351
- [“ip igmp startup-query-interval”](#) on page 1352
- [“ip igmp version”](#) on page 1353
- [“show debugging igmp”](#) on page 1354
- [“show ip igmp groups”](#) on page 1355
- [“show ip igmp interface”](#) on page 1357
- [“undebug igmp”](#) on page 1359

# clear ip igmp

**Overview** Use this command to clear all IGMP group membership records on all interfaces where it is configured .

**Syntax** `clear ip igmp`

**Mode** Privileged Exec

**Example** To delete all IGMP records, use the command

```
awplus# clear ip igmp
```

**Related commands**

- [clear ip igmp group](#)
- [clear ip igmp interface](#)
- [show ip igmp interface](#)
- [show running-config](#)

**Command changes**

- Version 5.4.7-1.1: VRF-lite support added SBx8100.
- Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.



# clear ip igmp group

**Overview** Use this command to clear IGMP group membership records for a specific group on either all interfaces, a single interface, or for a range of interfaces.

**Syntax** `clear ip igmp group *`  
`clear ip igmp group <ip-address> <interface>`

| Parameter    | Description                                                                                                    |
|--------------|----------------------------------------------------------------------------------------------------------------|
| *            | Clears all groups on all interfaces. This has the same effect as the <b>clear ip igmp</b> command.             |
| <ip-address> | Specifies the group whose membership records will be cleared from all interfaces, entered in the form A.B.C.D. |
| <interface>  | Specifies the name of the interface; all groups learned on this interface are deleted.                         |

**Mode** Privileged Exec

**Usage notes** This command applies to groups learned by IGMP.  
In addition to the group, an interface can be specified. Specifying this will mean that only entries with the group learned on the interface will be deleted.

**Examples** To delete all group records, use the command:

```
awplus# clear ip igmp group *
```

To delete records for 224.1.1.1 on eth0 use the command:

```
awplus# clear ip igmp group 224.1.1.1 eth0
```

**Related commands** [clear ip igmp](#)  
[clear ip igmp interface](#)  
[show ip igmp interface](#)  
[show running-config](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# clear ip igmp interface

**Overview** Use this command to clear IGMP group membership records on a particular interface.

**Syntax** `clear ip igmp interface <interface>`

| Parameter   | Description                                                                            |
|-------------|----------------------------------------------------------------------------------------|
| <interface> | Specifies the name of the interface. All groups learned on this interface are deleted. |

**Mode** Privileged Exec

**Usage notes** This command applies to interfaces configured for IGMP.

**Example** To delete records for eth0, use the command:  
`awplus# clear ip igmp interface eth0`

**Related commands**

- [clear ip igmp](#)
- [clear ip igmp group](#)
- [show ip igmp interface](#)
- [show running-config](#)

**Command changes**

- Version 5.4.7-1.1: VRF-lite support added SBx8100.
- Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# debug igmp

**Overview** Use this command to enable debugging of either all IGMP or a specific component of IGMP.

Use the **no** variant of this command to disable all IGMP debugging, or debugging of a specific component of IGMP.

**Syntax** `debug igmp {all|decode|encode|events|fsm|tib}`  
`no debug igmp {all|decode|encode|events|fsm|tib}`

| Parameter | Description                                   |
|-----------|-----------------------------------------------|
| all       | Enable or disable all debug options for IGMP  |
| decode    | Debug of IGMP packets that have been received |
| encode    | Debug of IGMP packets that have been sent     |
| events    | Debug IGMP events                             |
| fsm       | Debug IGMP Finite State Machine (FSM)         |
| tib       | Debug IGMP Tree Information Base (TIB)        |

**Modes** Privileged Exec and Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# debug igmp all`

**Related commands** [show debugging igmp](#)  
[undebug igmp](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip igmp

**Overview** Use this command to enable IGMP on an interface. The command configures the device as an IGMP querier.

Use the **no** variant of this command to return all IGMP related configuration to the default on this interface.

**Syntax** `ip igmp`  
`no ip igmp`

**Default** Disabled

**Mode** Interface Configuration for an Eth interface.

**Usage notes** An IP address must be assigned to the interface first, before this command will work.

**Example** To specify an interface as an IGMP querier, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp
```

**Related commands** [show ip igmp interface](#)  
[show running-config](#)

# ip igmp last-member-query-count

**Overview** Use this command to set the last-member query-count value for an interface.  
Use the **no** variant of this command to return to the default on an interface.

**Syntax** `ip igmp last-member-query-count <2-7>`  
`no ip igmp last-member-query-count`

| Parameter | Description                    |
|-----------|--------------------------------|
| <2-7>     | Last member query count value. |

**Default** The default last member query count value is 2.

**Mode** Interface Configuration for an Eth interface.

**Usage notes** This command applies to Eth interfaces configured for IGMP.

**Example** To set the last-member query-count to 3 on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp last-member-query-count 3
```

**Related commands** [ip igmp last-member-query-interval](#)  
[ip igmp startup-query-count](#)  
[show ip igmp interface](#)  
[show running-config](#)

# ip igmp last-member-query-interval

**Overview** Use this command to configure the frequency at which the router sends IGMP group specific host query messages.

Use the **no** variant of this command to set this frequency to the default.

**Syntax** `ip igmp last-member-query-interval <interval>`  
`no ip igmp last-member-query-interval`

| Parameter  | Description                                                                                                       |
|------------|-------------------------------------------------------------------------------------------------------------------|
| <interval> | The frequency in milliseconds at which IGMP group-specific host query messages are sent, in the range 1000-25500. |

**Default** 1000 milliseconds

**Mode** Interface Configuration for an Eth interface.

**Usage notes** This command applies to Eth interfaces configured for IGMP.

**Example** To change the IGMP group-specific host query message interval to 2 seconds (2000 milliseconds) on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp last-member-query-interval 2000
```

**Related commands** [ip igmp last-member-query-count](#)  
[show ip igmp interface](#)  
[show running-config](#)

# ip igmp mroute-proxy

**Overview** Use this command to enable IGMP mroute proxy on this downstream interface and associate it with the upstream proxy service interface.

Use the **no** variant of this command to remove the association with the proxy-service interface.

**Syntax** `ip igmp mroute-proxy <interface>`  
`no ip igmp mroute-proxy`

| Parameter   | Description                |
|-------------|----------------------------|
| <interface> | The name of the interface. |

**Mode** Interface Configuration for an Eth interface.

**Usage notes** This command applies to Eth interfaces configured for IGMP.

You must also enable the IGMP proxy service on the upstream interface, using the [ip igmp proxy-service](#) command. You can associate one or more downstream mroute proxy interfaces on the device with a single upstream proxy service interface. This downstream mroute proxy interface listens for IGMP reports, and forwards them to the upstream IGMP proxy service interface.

IGMP Proxy does not work with other multicast routing protocols, such as PIM-SM or PIM-DM.

**Example** To configure eth1 as the upstream proxy-service interface for the downstream eth0 interface, use the commands:

```
awplus# configure terminal
awplus(config)# ip multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ip igmp proxy-service
awplus(config-if)# ip igmp
awplus(config)# interface eth0
awplus(config-if)# ip igmp mroute-proxy eth1
awplus(config-if)# ip igmp
```

**Related commands** [ip igmp](#)  
[ip igmp proxy-service](#)  
[ip multicast-routing](#)

# ip igmp proxy-service

**Overview** Use this command to enable an interface to be the upstream IGMP proxy-service interface for the device. All associated downstream IGMP mroute proxy interfaces on this device will have their memberships consolidated on this proxy service interface, according to IGMP host-side functionality.

Use the **no** variant of this command to remove the designation of the interface as an upstream proxy-service interface.

**Syntax** `ip igmp proxy-service`  
`no ip igmp proxy-service`

**Mode** Interface Configuration for an Eth interface.

**Usage notes** This command applies to Eth interfaces configured for IGMP Proxy.

This command is used with the [ip igmp mroute-proxy](#) command to enable forwarding of IGMP reports to a proxy service interface for all forwarding entries for this interface. You must also enable the downstream IGMP mroute proxy interfaces on this device using the command [ip igmp mroute-proxy](#).

IGMP Proxy does not work with other multicast routing protocols, such as PIM-SM or PIM-DM.

From version 5.4.7-1.1 onwards, IGMP mroute proxy interfaces do not have to be configured with an IP address before they can operate. Instead, it is possible to have an addressless interface operate as an IGMP mroute proxy interface.

**Example** To configure eth1 as the upstream proxy-service interface for the downstream eth0 interface, use the commands:

```
awplus# configure terminal
awplus(config)# ip multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ip igmp proxy-service
awplus(config-if)# ip igmp
awplus(config)# interface eth0
awplus(config-if)# ip igmp mroute-proxy eth1
awplus(config-if)# ip igmp
```

**Related commands** [ip igmp](#)  
[ip igmp mroute-proxy](#)  
[ip multicast-routing](#)

**Command changes** Version 5.4.7-1.1: Addressless interface support added.  
Version 5.4.7-1.1: VRF-lite support added to SBx8100.  
Version 5.4.8-1.1: VRF-lite support added to x930, SBx908 GEN2.



# ip igmp querier-timeout

**Overview** Use this command to configure the timeout period before the device takes over as the querier for the interface after the previous querier has stopped querying.

Use the **no** variant of this command to restore the default.

**Syntax** `ip igmp querier-timeout <timeout>`  
`no ip igmp querier-timeout`

| Parameter | Description                                                           |
|-----------|-----------------------------------------------------------------------|
| <timeout> | IGMP querier timeout interval value in seconds, in the range 1-65535. |

**Default** The default timeout interval is 255 seconds.

**Mode** Interface Configuration for an Eth interface.

**Usage notes** This command applies to Eth interfaces configured for IGMP.  
The timeout value should not be less than the current active querier's general query interval.

**Example** To configure the device to wait 130 seconds from the time it received the last query before it takes over as the querier for eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp querier-timeout 130
```

**Related commands** [ip igmp query-interval](#)  
[show ip igmp interface](#)  
[show running-config](#)

# ip igmp query-holdtime

**Overview** This command sets the time that an IGMP Querier waits after receiving a query solicitation before it sends an IGMP Query. IGMP General Query messages will not be sent during the hold time interval.

Use the **no** variant of this command to return to the default query hold time period.

**Syntax** `ip igmp query-holdtime <interval>`  
`no ip igmp query-holdtime`

| Parameter  | Description                                                    |
|------------|----------------------------------------------------------------|
| <interval> | Query interval value in milliseconds, in the range <100-5000>. |

**Default** By default the delay before sending IGMP General Query messages is 500 milliseconds.

**Mode** Interface Configuration for an Eth interface.

**Usage notes** Use this command to configure a value for the IGMP query hold time in the current network. IGMP Queries can be generated after receiving Query Solicitation (QS) packets and there is a possibility of a DoS (Denial of Service) attack if a stream of Query Solicitation (QS) packets are sent to the IGMP Querier, eliciting a rapid stream of IGMP Queries. This command applies to interfaces on which the device is acting as an IGMP Querier.

Use the [ip igmp query-interval](#) command when a delay for IGMP general query messages is required and IGMP general query messages are required. The **ip igmp query-holdtime** command stops IGMP query messages during the configured holdtime interval, so the rate of IGMP Queries that can be sent out of an interface can be restricted.

See the [IGMP Feature Overview and Configuration Guide](#) for introductory information about the Query Solicitation feature.

**Examples** To set the IGMP query holdtime to 900 ms for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp query-holdtime 900
```

To reset the IGMP query holdtime to the default (500 ms) for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip igmp query-holdtime
```

**Related  
commands**

- `ip igmp query-interval`
- `show ip igmp interface`
- `show running-config`

# ip igmp query-interval

**Overview** Use this command to configure the period for sending IGMP General Query messages.

The IGMP query interval specifies the time between IGMP General Query messages being sent.

Use the **no** variant of this command to return to the default query interval period.

**NOTE:** The IGMP query interval must be greater than IGMP query maximum response time.

**Syntax** `ip igmp query-interval <interval>`  
`no ip igmp query-interval`

| Parameter  | Description                                              |
|------------|----------------------------------------------------------|
| <interval> | Query interval value in seconds, in the range <2-18000>. |

**Default** The default IGMP query interval is 125 seconds.

**Mode** Interface Configuration for an Eth interface.

**Usage notes** This command applies to interfaces configured for IGMP. Note that the IGMP query interval is automatically set to a greater value than the IGMP query max response time.

For example, if you set the IGMP query max response time to 2 seconds using the [ip igmp query-max-response-time](#) command, and the IGMP query interval is currently less than 3 seconds, then the IGMP query interval period will be automatically reconfigured to be 3 seconds, so it is greater than the IGMP query maximum response time.

Use the **ip igmp query-interval** command when a non-default interval for IGMP General Query messages is required.

The [ip igmp query-holdtime](#) command can occasionally delay the sending of IGMP Queries.

**Examples** To set the period between IGMP host-query messages to 3 minutes (180 seconds) for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp query-interval 180
```

To reset the period between sending IGMP host-query messages to the default (125 seconds) for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip igmp query-interval
```

**Related  
commands**

[ip igmp query-holdtime](#)  
[ip igmp query-max-response-time](#)  
[ip igmp startup-query-interval](#)  
[show ip igmp interface](#)  
[show running-config](#)

# ip igmp query-max-response-time

**Overview** Use this command to configure the maximum response time advertised in IGMP Queries.

Use the **no** variant of this command to restore the default.

**NOTE:** *The IGMP query maximum response time must be less than the IGMP query interval.*

**Syntax** `ip igmp query-max-response-time <response-time>`  
`no ip igmp query-max-response-time`

| Parameter                          | Description                                          |
|------------------------------------|------------------------------------------------------|
| <code>&lt;response-time&gt;</code> | Response time value in seconds, in the range 1-3180. |

**Default** The default IGMP query maximum response time is 10 seconds.

**Mode** Interface Configuration for an Eth interface.

**Usage notes** This command applies to interfaces configured for IGMP.  
Note that the IGMP query interval is automatically set to a greater value than the IGMP query maximum response time.

For example, if you set the IGMP query interval to 3 seconds using the [ip igmp query-interval](#) command, and the current IGMP query interval is less than 3 seconds, then the IGMP query maximum response time will be automatically reconfigured to be 2 seconds, so it is less than the IGMP query interval time.

To get the network to converge faster, use the **ip igmp query-max-response-time** command and set a low response time value, such as one or two seconds, so that the clients will respond immediately with a report as a response to the IGMP Queries.

**Examples** To set a maximum response time of 8 seconds for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp query-max-response-time 8
```

To reset the default maximum response time to the default (10 seconds) for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip igmp query-max-response-time
```

**Related  
commands**    `ip igmp query-interval`  
                  `show ip igmp interface`  
                  `show running-config`

## ip igmp ra-option

**Overview** Use this command to enable strict Router Alert (RA) option validation. With strict RA option enabled, IGMP packets without RA options are ignored.

Use the **no** variant of this command to disable strict RA option validation.

**Syntax** `ip igmp ra-option`  
`no ip igmp ra-option`

**Default** The default state of RA validation is unset.

**Mode** Interface Configuration for an Eth interface.

**Usage notes** This command applies to interfaces configured for IGMP and IGMP Snooping.

**Examples** To enable strict Router Alert (RA) option validation on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp ra-option
```



# ip igmp robustness-variable

**Overview** Use this command to change the robustness variable value on an interface.  
Use the **no** variant of this command to return to the default on an interface.

**Syntax** `ip igmp robustness-variable <1-7>`  
`no ip igmp robustness-variable`

| Parameter | Description                    |
|-----------|--------------------------------|
| <1-7>     | The robustness variable value. |

**Default** The default robustness variable value is 2.

**Mode** Interface Configuration for an Eth interface.

**Usage notes** This command applies to interfaces configured for IGMP.

**Examples** To set the robustness variable to 3 on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp robustness-variable 3
```

**Related commands** [show ip igmp interface](#)  
[show running-config](#)

# ip igmp source-address-check

**Overview** This command enables the checking of the Source Address for an IGMP Report, rejecting any IGMP Reports originating on devices outside of the local subnet.

Use the **no** variant of this command to disable the checking of the Source Address for an IGMP Report, which allows IGMP Reports from devices outside of the local subnet.

**Syntax** `ip igmp source-address-check`  
`no ip igmp source-address-check`

**Default** Source address checking for IGMP Reports is enabled by default.

**Mode** Interface Configuration for an Eth interface.

**Usage notes** This is a security feature, and should be enabled unless IGMP Reports from outside the local subnet are expected, for example, if Multicast VLAN Registration is active in the network.

The no variant of this command is required to disable the IGMP Report source address checking feature in networks that use Multicast VLAN Registration to allow IGMP Reports from devices outside of the local subnet.

**Examples** To deny IGMP Reports from outside the current subnet for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp source-address-check
```

To allow IGMP Reports from outside the current subnet for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip source-address-check
```

**Related commands** [show ip igmp interface](#)  
[show running-config](#)

# ip igmp startup-query-count

**Overview** Use this command to configure the IGMP startup query count for an interface. The IGMP startup query count is the number of IGMP General Query messages sent by a querier at startup. The default IGMP startup query count is 2.

Use the **no** variant of this command to return an interface's configured IGMP startup query count to the default.

**Syntax** `ip igmp startup-query-count <startup-query-count>`  
`no ip igmp startup-query-count`

| Parameter                                | Description                                              |
|------------------------------------------|----------------------------------------------------------|
| <code>&lt;startup-query-count&gt;</code> | Specify the IGMP startup query count, in the range 2-10. |

**Default** The default IGMP startup query count is 2.

**Mode** Interface Configuration for an Eth interface.

**Example** To set the IGMP startup query count to 4 on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp startup-query-count 4
```

**Related commands** [ip igmp last-member-query-count](#)  
[ip igmp startup-query-interval](#)

# ip igmp startup-query-interval

**Overview** Use this command to configure the IGMP startup query interval for an interface. The IGMP startup query interval is the amount of time in seconds between successive IGMP General Query messages sent by a querier during startup. The default IGMP startup query interval is one quarter of the IGMP query interval value.

Use the **no** variant of this command to return an interface's configured IGMP startup query interval to the default.

**Syntax** `ip igmp startup-query-interval <startup-query-interval>`  
`no ip igmp startup-query-interval`

| Parameter                                   | Description                                                                                                                              |
|---------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;startup-query-interval&gt;</code> | Specify the IGMP startup query interval, in the range of 2-1800 seconds. The value must be one quarter of the IGMP query interval value. |

**Default** The default IGMP startup query interval is one quarter of the IGMP query interval value.

**NOTE:** *The IGMP startup query interval must be one quarter of the IGMP query interval.*

**Mode** Interface Configuration for an Eth interface.

**Example** To set the IGMP startup query interval to 15 seconds for eth0, which is one quarter of the IGMP query interval of 60 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp query-interval 60
awplus(config-if)# ip igmp startup-query-interval 15
```

**Related commands** [ip igmp last-member-query-interval](#)  
[ip igmp query-interval](#)  
[ip igmp startup-query-count](#)

# ip igmp version

**Overview** Use this command to set the current IGMP version (IGMP version 1, 2 or 3) on an interface.

Use the **no** variant of this command to return to the default version.

**Syntax** `ip igmp version <1-3>`  
`no ip igmp version`

| Parameter                        | Description                  |
|----------------------------------|------------------------------|
| <code>version &lt;1-3&gt;</code> | IGMP protocol version number |

**Default** The default IGMP version is 3.

**Mode** Interface Configuration for an Eth interface.

**Example** To set the IGMP version to 2 for eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip igmp version 2
```

**Related commands** [show ip igmp interface](#)

# show debugging igmp

**Overview** Use this command to see what debugging is turned on for IGMP.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show debugging igmp`

**Mode** User Exec and Privileged Exec

**Example** To display the IGMP debugging options set, enter the command:

```
awplus# show debugging igmp
```

**Output** Figure 28-1: Example output from the **show debugging igmp** command

```
IGMP Debugging status:
IGMP Decoder debugging is on
IGMP Encoder debugging is on
IGMP Events debugging is on
IGMP FSM debugging is on
IGMP Tree-Info-Base (TIB) debugging is on
```

**Related commands** [debug igmp](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# show ip igmp groups

**Overview** Use this command to display the multicast groups with receivers directly connected to the router, and learned through IGMP.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip igmp groups [brief]`  
`show ip igmp groups <ip-address> [detail]`  
`show ip igmp groups <interface> [<ip-address>] [detail]`

| Parameter    | Description                                                  |
|--------------|--------------------------------------------------------------|
| <ip-address> | Address of the multicast group, entered in the form A.B.C.D. |
| <interface>  | Interface name for which to display local information.       |
| brief        | Brief display of all interfaces.                             |
| detail       | Detailed display of the interface.                           |

**Mode** User Exec and Privileged Exec

**Example** The following command displays local-membership information for all ports in all interfaces:

```
awplus# show ip igmp groups
```

**Output** Figure 28-2: Example output from **show ip igmp groups**

| IGMP Connected Group Membership |           |          |          |               |
|---------------------------------|-----------|----------|----------|---------------|
| Group Address                   | Interface | Uptime   | Expires  | Last Reporter |
| 224.0.1.1                       | eth0      | 00:00:09 | 00:04:17 | 10.10.0.82    |
| 224.0.1.24                      | eth1      | 00:00:06 | 00:04:14 | 10.10.0.84    |
| ...                             |           |          |          |               |

Table 28-1: Parameters in the output of **show ip igmp groups**

| Parameter     | Description                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------|
| Group Address | Address of the multicast group.                                                                              |
| Interface     | Port through which the group is reachable.                                                                   |
| Uptime        | The time in weeks, days, hours, minutes, and seconds that this multicast group has been known to the device. |

Table 28-1: Parameters in the output of **show ip igmp groups** (cont.)

| Parameter     | Description                                                    |
|---------------|----------------------------------------------------------------|
| Expires       | Time (in hours, minutes, and seconds) until the entry expires. |
| Last Reporter | Last host to report being a member of the multicast group.     |

**Command  
changes**

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

Version 5.4.8-2.3: **brief** parameter added.



# show ip igmp interface

**Overview** Use this command to display the state of IGMP for a specified interface. IGMP is shown as Active or Disabled in the show output.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show ip igmp interface [<interface>]

| Parameter   | Description                |
|-------------|----------------------------|
| <interface> | The name of the interface. |

**Mode** User Exec and Privileged Exec

**Output** The following output shows IGMP interface status for an eth0 interface.

```
awplus#show ip igmp interface

Interface eth0 (Index 3)
 IGMP Disabled, Inactive, Non-Querier, Version 3 (default)
 Internet address is 172.22.0.2
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP querying router is 0.0.0.0
 IGMP robustness variable is 2
 IGMP query interval is 125 seconds
 IGMP Startup query interval is 31 seconds
 IGMP Startup query count is 2
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Group Membership interval is 260 seconds
 IGMP last member query count is 2
 Last member query response interval is 1000 milliseconds
 Strict IGMPv3 ToS checking is disabled on this interface
 Source Address checking is enabled
 Global Specific Query Flooding is enabled
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally enabled for
Root/Master Nodes
 IGMP Snooping query solicitation is globally disabled for Non
Root/Master Nodes
 Num. query-solicit packets: 0 sent, 0 recvd
 IGMP Snooping is not enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
 IGMP Snooping source timer is globally disabled
 IGMP Snooping source timer is disabled
```

**Command  
changes**

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# undebbug igmp

**Overview** This command applies the functionality of the no [debug igmp](#) command.

# 29

# MLD Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of configuration, clear, and show commands related to MLD and MLD Snooping.

The Multicast Listener Discovery (MLD) module includes the MLD Proxy service and MLD Snooping functionality. Some of the following commands may have commonalities and restrictions; these are described under the Usage section for each command.

MLD and MLD Snooping commands only apply to switch ports, not Ethernet interfaces.

Before using PIM-SMv6:

- IPv6 must be enabled on an interface ([ipv6 enable](#)),
- IPv6 forwarding must be enabled globally for routing IPv6 ([ipv6 forwarding](#)), and
- IPv6 multicasting must be enabled globally ([ipv6 multicast-routing](#)).

- Command List**
- [“clear ipv6 mld”](#) on page 1362
  - [“clear ipv6 mld group”](#) on page 1363
  - [“clear ipv6 mld interface”](#) on page 1364
  - [“debug mld”](#) on page 1365
  - [“ipv6 mld”](#) on page 1366
  - [“ipv6 mld last-member-query-count”](#) on page 1367
  - [“ipv6 mld last-member-query-interval”](#) on page 1368
  - [“ipv6 mld querier-timeout”](#) on page 1369
  - [“ipv6 mld query-interval”](#) on page 1370
  - [“ipv6 mld query-max-response-time”](#) on page 1371
  - [“ipv6 mld robustness-variable”](#) on page 1372

- [“ipv6 mld static-group”](#) on page 1373
- [“ipv6 mld version”](#) on page 1374
- [“show debugging mld”](#) on page 1375
- [“show ipv6 mld groups”](#) on page 1376
- [“show ipv6 mld interface”](#) on page 1378

# clear ipv6 mld

**Overview** Use this command to clear all MLD local memberships on all interfaces.

**Syntax** `clear ipv6 mld`

**Mode** Privileged Exec

**Example** To clear all MLD local memberships on all interfaces, use the command:

```
awplus# clear ipv6 mld
```

**Related commands** [clear ipv6 mld group](#)  
[clear ipv6 mld interface](#)

# clear ipv6 mld group

**Overview** Use this command to clear MLD specific local-membership(s) on all interfaces, for all groups or a particular group.

**Syntax** `clear ipv6 mld group {*|<ipv6-address>}`

| Parameter      | Description                                                                                                                                                                        |
|----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| *              | Clears all groups on all interfaces. This is an alias to the <a href="#">clear ipv6 mld</a> command.                                                                               |
| <ipv6-address> | Specify the group address for which MLD local-memberships are to be cleared from all interfaces.<br>Specify the IPv6 multicast group address in the format in the format X:X::X:X. |

**Mode** Privileged Exec

**Example** To clear all groups on all interfaces, use the command:

```
awplus# clear ipv6 mld group *
```

**Related commands** [clear ipv6 mld](#)  
[clear ipv6 mld interface](#)

# clear ipv6 mld interface

**Overview** Use this command to clear MLD interface entries.

**Syntax** `clear ipv6 mld interface <interface>`

| Parameter                      | Description                                                                          |
|--------------------------------|--------------------------------------------------------------------------------------|
| <code>&lt;interface&gt;</code> | Specifies name of the interface; all groups learned from this interface are deleted. |

**Mode** Privileged Exec

**Example** To clear the entries from eth1, use the command:

```
awplus# clear ipv6 mld interface eth1
```

**Related commands** [clear ipv6 mld](#)  
[clear ipv6 mld group](#)



# debug mld

**Overview** Use this command to enable all MLD debugging modes, or a specific MLD debugging mode.

Use the **no** variant of this command to disable all MLD debugging modes, or a specific MLD debugging mode.

**Syntax** `debug mld {all|decode|encode|events|fsm|tib}`  
`no debug mld {all|decode|encode|events|fsm|tib}`

| Parameter | Description                            |
|-----------|----------------------------------------|
| all       | Debug all MLD.                         |
| decode    | Debug MLD decoding.                    |
| encode    | Debug MLD encoding.                    |
| events    | Debug MLD events.                      |
| fsm       | Debug MLD Finite State Machine (FSM).  |
| tib       | Debug MLD Tree Information Base (TIB). |

**Mode** Privileged Exec and Global Configuration

**Examples**

```
awplus# configure terminal
awplus(config)# debug mld all
awplus# configure terminal
awplus(config)# debug mld decode
awplus# configure terminal
awplus(config)# debug mld encode
awplus# configure terminal
awplus(config)# debug mld events
```

**Related commands** [show debugging mld](#)

# ipv6 mld

**Overview** Use this command to enable the MLD protocol operation on an interface. This command enables MLD protocol operation in stand-alone mode, and can be used to learn local-membership information prior to enabling a multicast routing protocol on the interface.

Use the **no** variant of this command to return all MLD related configuration to the default.

**Syntax** `ipv6 mld`  
`no ipv6 mld`

**Default** MLD is disabled by default.

**Mode** Interface Configuration for a specified Eth interface or a range of Eth interfaces.

**Usage notes** MLD requires memory for storing data structures, as well as the hardware tables to implement hardware routing. As the number of ports increases then more memory is consumed. You can track the memory used for MLD with the command:

```
awplus# show memory pools nsm | grep MLD
```

**Example** To enable MLD on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld
```

**Related commands** [show ipv6 mld interface](#)

# ipv6 mld last-member-query-count

**Overview** Use this command to set the last-member query-count value.  
Use the **no** variant of this command to return to the default on an interface.

**Syntax** `ipv6 mld last-member-query-count <value>`  
`no ipv6 mld last-member-query-count`

| Parameter | Description                                |
|-----------|--------------------------------------------|
| <value>   | Count value. Valid values are from 2 to 7. |

**Default** The default last-member query-count value is 2.

**Mode** Interface Configuration for a specified Eth interface or a range of Eth interfaces.

**Example** To set the last-member query-count to 3 on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld last-member-query-count 3
```

# ipv6 mld last-member-query-interval

**Overview** Use this command to configure the interval at which the router sends MLD group-specific host query messages.

Use the **no** variant of this command to set this frequency to the default.

**Syntax** `ipv6 mld last-member-query-interval <milliseconds>`  
`no ipv6 mld last-member-query-interval`

| Parameter                         | Description                                                                                                           |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <code>&lt;milliseconds&gt;</code> | The time delay between successive query messages (in milliseconds). Valid values are from 1000 to 25500 milliseconds. |

**Default** 1000 milliseconds

**Mode** Interface Configuration for a specified Eth interface or a range of Eth interfaces.

**Example** The following example changes the MLD group-specific host query message interval to 2 seconds:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld last-member-query-interval 2000
```

# ipv6 mld querier-timeout

**Overview** Use this command to configure the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

Use the **no** variant of this command to restore the default.

**Syntax** `ipv6 mld querier-timeout <seconds>`  
`no ipv6 mld querier-timeout`

| Parameter | Description                                                                                                                                                            |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <seconds> | Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier. Valid values are from 2 to 65535 seconds. |

**Default** 255 seconds

**Mode** Interface Configuration for a specified Eth interface or a range of Eth interfaces.

**Usage notes** This command applies to interfaces configured for MLD Layer 3 multicast protocols.

**Example** The following example configures the router to wait 120 seconds from the time it received the last query before it takes over as the querier for the interface:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld querier-timeout 120
```

**Related commands** [ipv6 mld query-interval](#)

# ipv6 mld query-interval

**Overview** Use this command to configure the frequency of sending MLD host query messages.

Use the **no** variant of this command to return to the default frequency.

**Syntax** `ipv6 mld query-interval <seconds>`  
`no ipv6 mld query-interval`

| Parameter | Description                                                                                                                               |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <seconds> | Variable that specifies the time delay between successive MLD host query messages (in seconds). Valid values are from 1 to 18000 seconds. |

**Default** The default query interval is 125 seconds.

**Mode** Interface Configuration for a specified Eth interface or a range of Eth interfaces.

**Usage** This command applies to interfaces configured for MLD Layer 3 multicast protocols.

**Example** The following example changes the frequency of sending MLD host-query messages to 2 minutes:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld query-interval 120
```

**Related commands** [ipv6 mld querier-timeout](#)

# ipv6 mld query-max-response-time

**Overview** Use this command to configure the maximum response time advertised in MLD queries.

Use the **no** variant of with this command to restore the default.

**Syntax** `ipv6 mld query-max-response-time <seconds>`  
`no ipv6 mld query-max-response-time`

| Parameter | Description                                                                                              |
|-----------|----------------------------------------------------------------------------------------------------------|
| <seconds> | Maximum response time (in seconds) advertised in MLD queries.<br>Valid values are from 1 to 240 seconds. |

**Default** 10 seconds

**Mode** Interface Configuration for a specified Eth interface or a range of Eth interfaces.

**Usage** This command applies to interfaces configured for MLD Layer 3 multicast protocols.

**Example** The following example configures a maximum response time of 8 seconds:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld query-max-response-time 8
```

# ipv6 mld robustness-variable

**Overview** Use this command to change the robustness variable value on an interface.  
Use the **no** variant of this command to return to the default on an interface.

**Syntax** `ipv6 mld robustness-variable <value>`  
`no ipv6 mld robustness-variable`

| Parameter | Description                   |
|-----------|-------------------------------|
| <value>   | Valid values are from 1 to 7. |

**Default** The default robustness variable value is 2.

**Mode** Interface Configuration for a specified Eth interface or a range of Eth interfaces.

**Usage** This command applies to interfaces configured for MLD Layer 3 multicast protocols.

**Example** The following example changes the robustness variable value to 3:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld robustness-variable 3
```



# ipv6 mld static-group

**Overview** Use this command to statically configure IPv6 group membership entries on an interface. To statically add only a group membership, do not specify any parameters.

Use the **no** variant of this command to delete static group membership entries.

**Syntax** `ipv6 mld static-group <ipv6-group-address> [source <ipv6-source-address>] [interface <port>]`  
`no ipv6 mld static-group <ipv6-group-address> [source <ipv6-source-address>] [interface <port>]`

| Parameter                                | Description                                                                                                                                                                                                                                                                |
|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-group-address&gt;</code>  | Specify a standard IPv6 Multicast group address to be configured as a static group member. The IPv6 address uses the format X:X::X:X.                                                                                                                                      |
| <code>&lt;ipv6-source-address&gt;</code> | Optional. Specify a standard IPv6 source address to be configured as a static source from where multicast packets originate. The IPv6 address uses the format X:X::X:X.                                                                                                    |
| <code>&lt;port&gt;</code>                | Optional. Physical interface. This parameter specifies a physical port. If this parameter is used, the static configuration is applied to just that physical interface. If this parameter is not used, the static configuration is applied on all interfaces in the group. |

**Mode** Interface Configuration for a specified Eth interface.

**Examples** To add a static group record, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 mld static-group ff1e::10
```

To add a static group and source record, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 mld static-group ff1e::10 source
fe80::2fd:6cff:felc:b
```

# ipv6 mld version

**Overview** Use this command to set the current MLD protocol version on an interface.  
Use the **no** variant of this command to return to the default version on an interface.

**Syntax** `ipv6 mld version <version>`  
`no ipv6 mld version`

| Parameter | Description                                                    |
|-----------|----------------------------------------------------------------|
| <version> | MLD protocol version number. Valid version numbers are 1 and 2 |

**Default** The default MLD protocol version number is 2.

**Mode** Interface Configuration for a specified Eth interface.

**Usage notes** Note this command is intended for use where there is another querier (when there is another device with MLD enabled) on the same link that can only operate with MLD version 1. Otherwise, the default MLD version 2 is recommended for performance.

**Example** To set the MLD protocol version to 1, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld version 1
```

# show debugging mld

**Overview** Use this command to see what debugging is turned on for MLD. MLD debugging modes are enabled with the [debug mld](#) command.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show debugging mld`

**Mode** Privileged Exec

**Example** `awplus# show debugging mld`

## Output

```
show debugging mld
MLD Debugging status:
 MLD Decoder debugging is on
 MLD Encoder debugging is on
 MLD Events debugging is on
 MLD FSM debugging is on
 MLD Tree-Info-Base (TIB) debugging is on
```

**Related commands** [debug mld](#)

# show ipv6 mld groups

**Overview** Use this command to display the multicast groups that have receivers directly connected to the router and learned through MLD.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 mld groups [<ipv6-address>|<interface>] [detail]`

| Parameter      | Description                                                                 |
|----------------|-----------------------------------------------------------------------------|
| <ipv6-address> | Optional.<br>Specify the address of the multicast group in format X:X::X:X. |
| <interface>    | Optional.<br>The interface to display information about.                    |
| detail         | Display more detailed information.                                          |

**Mode** User Exec and Privileged Exec

**Examples** The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups
```

The following command displays detailed local-membership information for all interfaces:

```
awplus# show ipv6 mld groups detail
```

**Output** Figure 29-1: Example output for **show ipv6 mld groups**

```
awplus#show ipv6 mld groups
MLD Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
ff03::1 eth3 00:00:37 00:03:43 fe80::214:1ff:fe00:1
ff03::2 eth3 00:00:37 00:03:43 fe80::214:1ff:fe00:1
```

Figure 29-2: Example output for **show ipv6 mld groups detail**

```
awplus# show ipv6 mld groups detail
MLD Connected Group Membership Details for eth3
Interface: eth3
Group: ff03::1
Uptime: 00:00:37
Group mode: Include ()
Last reporter: fe80::214:1ff:fe00:1
Group source list: (R - Remote, M - SSM Mapping, S - Static)
Source Address Uptime v2 Exp Fwd Flags
2001:db8::1 00:00:37 00:03:43 Yes R
2002:db8::3 00:00:37 00:03:43 Yes R
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 mld interface

**Overview** Use this command to display the state of MLD and MLD Snooping for a specified interface, or all interfaces.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 mld interface [<interface>]`

| Parameter   | Description                                            |
|-------------|--------------------------------------------------------|
| <interface> | Optionally, an interface to display information about. |

**Mode** User Exec and Privileged Exec

**Example** The following command displays MLD interface status on all interfaces enabled for MLD:

```
awplus# show ipv6 mld interface
```

**Output** Figure 29-3: Example output for **show ipv6 mld interface**

```
awplus#show ipv6 mld interface

Interface eth3 (Index 15)
 MLD Enabled, Active, Querier, Version 2 (default)
 Internet address is 2001:abcd:cafe:4::2
 MLD interface has 2 group-record states
 MLD activity: 172 joins, 162 leaves
 MLD robustness variable is 2
 MLD last member query count is 2
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 MLD Snooping is globally enabled
 MLD Snooping is not enabled on this interface
 MLD Snooping fast-leave is not enabled
 MLD Snooping querier is not enabled
 MLD Snooping report suppression is enabled
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# 30

# Multicast Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of multicast commands for configuring:

- IPv4 and IPv6 multicast forwarding
- IPv4 and IPv6 static multicast routes
- mroutes (routes back to a multicast source)

For commands for other multicast protocols, see:

- [IGMP Commands](#)
- [MLD Commands](#)
- [PIM-SM Commands](#)
- [PIM-SMv6 Commands](#)

**NOTE:** Before using PIM-SMv6 commands, IPv6 must be enabled on an interface with the [ipv6 enable](#) command, IPv6 forwarding must be enabled globally for routing IPv6 with the [ipv6 forwarding](#) command, and IPv6 multicasting must be enabled globally with the [ipv6 multicast-routing](#) command.

Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the [clear ipv6 mroute](#) command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.

The IPv6 Multicast addresses shown can be derived from IPv6 unicast prefixes as per RFC 3306. The IPv6 unicast prefix reserved for documentation is 2001:0db8::/32 as per RFC 3849. Using the base /32 prefix the IPv6 multicast prefix for 2001:0db8::/32 is ff3x:20:2001:0db8::/64. Where an RP address is 2001:0db8::1 the embedded RP multicast prefix is ff7x:120:2001:0db8::/96.

The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.

- Command List**
- “clear ip mroute” on page 1381
  - “clear ip mroute statistics” on page 1383
  - “clear ip multicast route” on page 1384
  - “clear ipv6 mroute” on page 1385
  - “clear ipv6 mroute statistics” on page 1386
  - “debug nsm” on page 1387
  - “debug nsm mcast” on page 1388
  - “debug nsm mcast6” on page 1389
  - “ip mroute” on page 1390
  - “ip multicast handle-igmp-immediately” on page 1392
  - “ip multicast route” on page 1393
  - “ip multicast route-limit” on page 1395
  - “ip multicast wrong-vif-suppression” on page 1396
  - “ip multicast-routing” on page 1397
  - “ipv6 mroute” on page 1398
  - “ipv6 multicast route” on page 1400
  - “ipv6 multicast route-limit” on page 1402
  - “ipv6 multicast-routing” on page 1403
  - “show debugging nsm mcast” on page 1404
  - “show ip mroute” on page 1405
  - “show ip mvif” on page 1408
  - “show ip rpf” on page 1409
  - “show ipv6 mif” on page 1410
  - “show ipv6 mroute” on page 1411
  - “show ipv6 multicast forwarding” on page 1413



# clear ip mroute

**Overview** Use this command to delete one or more dynamically-added route entries from the IPv4 multicast routing table.

You need to do this if, for example, you want to create a static route instead of an existing dynamic route.

**NOTE:** If you use this command, you should also use the [clear ip igmp group](#) command to clear IGMP group membership records.

**Syntax** `clear ip mroute {*|<ipv4-group-address>  
[<ipv4-source-address>]} [pim sparse-mode]`

| Parameter             | Description                                                            |
|-----------------------|------------------------------------------------------------------------|
| *                     | Deletes all dynamically-learned IPv4 multicast routes.                 |
| <ipv4-group-address>  | Group IPv4 address, in dotted decimal notation in the format A.B.C.D.  |
| <ipv4-source-address> | Source IPv4 address, in dotted decimal notation in the format A.B.C.D. |
| pim sparse-mode       | Clear specified IPv4 multicast route(s) for PIM Sparse Mode only.      |

**Mode** Privileged Exec

**Usage notes** When this command is used, the Multicast Routing Information Base (MRIB) clears the specified dynamic IPv4 multicast route entries in its IPv4 multicast route table, and deletes the entries from the multicast forwarder. The MRIB also sends a “clear” message to the relevant multicast protocols.

This command does not delete static routes from the routing table or the configuration. To delete static routes, use the **no** parameter of the command [ip multicast route](#), or the command [clear ip multicast route](#).

**Examples** To delete a specific dynamic route (from 192.168.3.3 for the group 225.1.1.1), use the command:

```
awplus# clear ip mroute 225.1.1.1 192.168.3.3
```

To delete all dynamic multicast routes, use the command:

```
awplus# clear ip mroute *
```

**Related commands** [clear ip multicast route](#)  
[ip multicast route](#)  
[show ip mroute](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# clear ip mroute statistics

**Overview** Use this command to delete multicast route statistics entries from the IP multicast routing table.

**Syntax** `clear ip mroute statistics {*|<ipv4-group-addr>  
[<ipv4-source-addr>]}`

| Parameter             | Description                                                            |
|-----------------------|------------------------------------------------------------------------|
| *                     | Deletes all dynamically-learned IPv4 multicast routes.                 |
| <ipv4-group-address>  | Group IPv4 address, in dotted decimal notation in the format A.B.C.D.  |
| <ipv4-source-address> | Source IPv4 address, in dotted decimal notation in the format A.B.C.D. |

**Mode** Privileged Exec

**Example** `awplus# clear ip mroute statistics 225.1.1.2 192.168.4.4`  
`awplus# clear ip mroute statistics *`

# clear ip multicast route

**Overview** Use this command to delete all user-added static IPv4 multicast routes.

**Syntax** `clear ip multicast route *`

| Parameter | Description                               |
|-----------|-------------------------------------------|
| *         | Deletes all static IPv4 multicast routes. |

**Mode** Privileged Exec

**Usage notes** This command deletes all static IPv4 multicast routes from the routing table. To delete a single static route, use the **no** parameter of the command [ip multicast route](#). To delete dynamic routes, use the command [clear ip mroute](#).

**Example** To delete all static IPv4 multicast route entries, use the command:

```
awplus# clear ip multicast route *
```

**Related commands**

- [clear ip mroute](#)
- [ip multicast route](#)
- [show ip mroute](#)

# clear ipv6 mroute

**Overview** Use this command to delete one or more dynamically-added route entries from the IPv6 multicast routing table.

You need to do this if, for example, you want to create a static route instead of an existing dynamic route.

**NOTE:** If you use this command, you should also use the [clear ipv6 mld group](#) command to clear MLD group membership records.

**Syntax** `clear ipv6 mroute {*|<ipv6-group-address>  
[<ipv6-source-address>]} [pim sparse-mode]`

| Parameter             | Description                                                          |
|-----------------------|----------------------------------------------------------------------|
| *                     | Deletes all dynamically-learned IPv6 multicast routes.               |
| <ipv6-group-address>  | Group IPv6 address, in hexadecimal notation in the format X.X::X.X.  |
| <ipv6-source-address> | Source IPv6 address, in hexadecimal notation in the format X.X::X.X. |
| pim sparse-mode       | Clear specified IPv6 multicast route(s) for PIM Sparse Mode only.    |

**Mode** Privileged Exec

**Usage notes** When this command is used, the Multicast Routing Information Base (MRIB) clears the specified dynamic IPv6 multicast route entries in its IPv6 multicast route table, and deletes the entries from the multicast forwarder. The MRIB also sends a “clear” message to the relevant multicast protocols.

This command does not delete static routes from the routing table or the configuration. To delete static routes, use the **no** parameter of the command [ipv6 multicast route](#).

**Examples** To delete a specific dynamic route (from ff08::1 for the group 2001::2), use the command:

```
awplus# clear ipv6 mroute 2001::2 ff08::1
```

To delete all dynamic multicast routes, use the command:

```
awplus# clear ipv6 mroute *
```

**Related commands** [ipv6 multicast route](#)  
[show ipv6 mroute](#)

# clear ipv6 mroute statistics

**Overview** Use this command to delete multicast route statistics entries from the IPv6 multicast routing table.

**Syntax** `clear ipv6 mroute statistics {*|<ipv6-group-address> [<ipv6-source-address>]}`

| Parameter          | Description                                                          |
|--------------------|----------------------------------------------------------------------|
| *                  | All multicast route entries.                                         |
| <ipv6-group-addr>  | Group IPv6 address, in hexadecimal notation in the format X.X::X.X.  |
| <ipv6-source-addr> | Source IPv6 address, in hexadecimal notation in the format X.X::X.X. |

**Mode** Privileged Exec

**Examples** `awplus# clear ipv6 mroute statistics 2001::2 ff08::1`  
`awplus# clear ipv6 mroute statistics *`

# debug nsm

**Overview** This command specifies a set of debug options for use by Allied Telesis authorized service personnel only.

Use the **no** variant of this command to remove debug options.

**Syntax** `debug nsm [all|events|ha|kernel]`  
`no debug nsm [all|events|ha|kernel]`

| Parameter | Description                                         |
|-----------|-----------------------------------------------------|
| all       | Enables all the nsm debugging options               |
| events    | Enables the nsm events debugging options            |
| ha        | Enables the nsm high availability debugging options |
| kernel    | Enables the nsm kernel debugging options            |

**Mode** Global Configuration, Privileged Exec

**Usage notes** This command is intended for use by Allied Telesis authorized service personnel for diagnostic purposes.

**Related commands** [show debugging nsm mcast](#)

**Command changes** Version 5.4.7-2.1 command added.

# debug nsm mcast

**Overview** Use this command to debug IPv4 events in the Multicast Routing Information Base (MRIB).

This command is intended for use by Allied Telesis authorized service personnel for diagnostic purposes.

**Syntax** `debug nsm mcast`  
`{all|fib-msg|mrt|mtrace|mtrace-detail|register|stats|vif}`

| Parameter     | Description                                 |
|---------------|---------------------------------------------|
| all           | All IPv4 multicast debugging.               |
| fib-msg       | Forwarding Information Base (FIB) messages. |
| mrt           | Multicast routes.                           |
| mtrace        | Multicast traceroute.                       |
| mtrace-detail | Multicast traceroute detailed debugging.    |
| register      | Multicast PIM register messages.            |
| stats         | Multicast statistics.                       |
| vif           | Multicast interface.                        |

**Mode** Privileged Exec and Global Configuration

**Examples** To enable debugging of all multicast route events, use the commands:

```
awplus# configure terminal
awplus(config)# debug nsm mcast all
```

To enable debugging of PIM register entries, use the commands:

```
awplus# configure terminal
awplus(config)# debug nsm mcast register
```

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.



# debug nsm mcast6

**Overview** Use this command to debug IPv6 events in the Multicast Routing Information Base (MRIB).

This command is intended for use by Allied Telesis authorized service personnel for diagnostic purposes.

**Syntax** `debug nsm mcast6 {all|fib-msg|mrt|register|stats|vif}`  
`no debug nsm mcast6 {all|fib-msg|mrt|register|stats|vif}`

| Parameter | Description                                 |
|-----------|---------------------------------------------|
| all       | All IPv6 multicast route debugging.         |
| fib-msg   | Forwarding Information Base (FIB) messages. |
| mrt       | Multicast routes.                           |
| register  | Multicast PIM register messages.            |
| stats     | Multicast statistics.                       |
| vif       | Multicast interfaces.                       |

**Mode** Privileged Exec and Global Configuration

**Examples** To enable debugging of all multicast route events, use the commands:

```
awplus# configure terminal
awplus(config)# debug nsm mcast6 all
```

To enable debugging of PIM register entries, use the commands:

```
awplus# configure terminal
awplus(config)# debug nsm mcast6 register
```

# ip mroute

**Overview** Use this command to inform multicast of the RPF (Reverse Path Forwarding) route to a given IPv4 multicast source.

Use the **no** variant of this command to delete a route to an IPv4 multicast source.

**Syntax** `ip mroute <ipv4-source-address/mask-length>  
[bgp|ospf|rip|static] <rpf-address> [<admin-distance>]`

| Parameter                                            | Description                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv4-source-address/mask-length&gt;</code> | A multicast source IPv4 address and mask length, in dotted decimal notation in the format A.B.C.D/M.                                                                                                                                                                                                                                           |
| <code>bgp</code>                                     | BGP unicast routing protocol.                                                                                                                                                                                                                                                                                                                  |
| <code>ospf</code>                                    | OSPF unicast routing protocol.                                                                                                                                                                                                                                                                                                                 |
| <code>rip</code>                                     | RIP unicast routing protocol.                                                                                                                                                                                                                                                                                                                  |
| <code>static</code>                                  | Specifies a static route.                                                                                                                                                                                                                                                                                                                      |
| <code>&lt;rpf-address&gt;</code>                     | A.B.C.D<br>The closest known address on the multicast route back to the specified source. This host IPv4 address can be within a directly connected subnet or within a remote subnet. In the case that the address is in a remote subnet, a lookup is done from the unicast route table to find the next hop address on the path to this host. |
| <code>&lt;admin-distance&gt;</code>                  | The administrative distance. Use this to determine whether the RPF lookup selects the unicast or multicast route. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence. The default is 0 and the range available is 0-255.               |

**Mode** Global Configuration

**Usage notes** Typically, when a Layer 3 multicast routing protocol is determining the RPF (Reverse Path Forwarding) interface for the path to an IPv4 multicast source, it uses the unicast route table to find the best path to the source. However, in some networks a deliberate choice is made to send multicast via different paths to those used for unicast. In this case, the interface via which a multicast stream from a given source enters a router may not be the same as the interface that connects to the best unicast route to that source.

This command enables the user to statically configure the device with "multicast routes" back to given sources. When performing the RPF check on a stream from a given IPv4 source, the multicast routing protocol will look at these static entries as well as looking into the unicast routing table. The route with the lowest administrative distance - whether a static "multicast route" or a route from the unicast route table - will be chosen as the RPF route to the source.

Note that in this context the term “multicast route” does not imply a route via which the current router will forward multicast; instead it refers to the route the multicast will have traversed in order to arrive at the current router.

**Examples** The following example creates a static multicast IPv4 route back to the sources in the 10.10.3.0/24 subnet. The multicast route is via the host 192.168.2.3, and has an administrative distance of 2:

```
awplus# configure terminal
awplus(config)# ip mroute 10.10.3.0/24 static 2 192.168.2.3 2
```

The following example creates a static multicast IPv4 route back to the sources in the 192.168.3.0/24 subnet. The multicast route is via the host 10.10.10.50. The administrative distance on this route has the default value of 0:

```
awplus# configure terminal
awplus(config)# ip mroute 192.168.3.0/24 10.10.10.50
```

**Validation  
Commands**

- clear ip mroute
- show ip mroute
- show ip rpf

# ip multicast handle-igmp-immediately

**Overview** Use this command to allow traffic to be switched as soon as an IGMP report is received.

Use the **no** variant of this command to revert to the default setting.

**Syntax** `ip multicast handle-igmp-immediately`  
`no ip multicast handle-igmp-immediately`

**Default** Turned off. This means that traffic will be switched after either a 1 second delay or if the IGMP buffer fills with 250 packets.

**Mode** Global Configuration

**Example** To turn on this feature, use the commands:

```
awplus# configure terminal
awplus(config)# ip multicast handle-igmp-immediately
```

**Related commands** [show running-config](#)

**Command changes** Supported since software version 5.4.9-2.0

# ip multicast route

**Overview** Use this command to add an IPv4 static multicast route for a specific multicast source and group IPv4 address to the multicast Routing Information Base (RIB). This IPv4 multicast route is used to forward multicast traffic from a specific source and group ingressing on an upstream interface to a single or range of downstream interfaces.

Use the **no** variant of this command to either remove an IPv4 static multicast route set with this command or to remove a specific downstream interface from an IPv4 static multicast route for a specific multicast source and group IPv4 address.

**Syntax**

```
ip multicast route <ipv4-source-addr> <ipv4-group-addr>
<upstream-interface> [<downstream-interface>]

no ip multicast route <ipv4-source-addr> <ipv4-group-addr>
[<upstream-interface> <downstream-interface>]
```

| Parameter              | Description                                                                          |
|------------------------|--------------------------------------------------------------------------------------|
| <ipv4-source-addr>     | Source IPv4 address, in dotted decimal notation in the format A.B.C.D.               |
| <ipv4-group-addr>      | Group IPv4 address, in dotted decimal notation in the format A.B.C.D.                |
| <upstream-interface>   | Upstream interface on which the multicast packets ingress.                           |
| <downstream-interface> | Downstream interface or range of interfaces to which the multicast packets are sent. |

**Default** By default, this feature is disabled.

**Mode** Global Configuration

**Usage notes** Only one multicast route entry per IPv4 address and multicast group can be specified. Therefore, if one entry for a static multicast route is configured, PIM will not be able to update this multicast route in any way.

If a dynamic multicast route exists you cannot create a static multicast route with the same source IPv4 address, group IPv4 address, upstream interface and downstream interfaces. An error message is displayed and logged. To add a new static multicast route, either wait for the dynamic multicast route to timeout or clear the dynamic multicast route with the [clear ip mroute](#) command.

To update an existing static multicast route entry with more or a new set of downstream interfaces, you must first remove the existing static multicast route and then add the new static multicast route with all downstream interfaces specified. If you attempt to update an existing static multicast route entry with an additional interface or interfaces, an error message is displayed and logged.

To create a blackhole or null route where packets from a specified source and group address coming from an upstream interface are dropped rather than

forwarded, do not specify the optional *<downstream-interface>* parameter when entering this command.

To remove a specific downstream interface from an existing static multicast route entry, specify the interface you want to remove with the *<downstream-interface>* parameter when entering the **no** variant of this command.

**Examples** To create a static multicast route for the multicast source IPv4 address 2.2.2.2 and group IPv4 address 224.9.10.11, specifying the upstream Eth interface as eth0 and the downstream interface as eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11 eth0
eth1
```

To create a blackhole route for the multicast source IPv4 address 2.2.2.2 and group IPv4 address 224.9.10.11, specifying the upstream interface as eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11 eth0
```

To delete an IPv4 static multicast route for the multicast source IP address 2.2.2.2 and group IP address 224.9.10.11, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast route 2.2.2.2 224.9.10.11
```

**Related commands**

- [clear ip mroute](#)
- [clear ip multicast route](#)
- [show ip mroute](#)

# ip multicast route-limit

**Overview** Use this command to limit the number of multicast routes that can be added to an IPv4 multicast routing table.

Use the **no** variant of this command to return the IPv4 route limit to the default.

**Syntax** `ip multicast route-limit <limit> [<threshold>]`  
`no ip multicast route-limit`

| Parameter   | Description                                                                                                                        |
|-------------|------------------------------------------------------------------------------------------------------------------------------------|
| <limit>     | <1-2147483647> Number of routes.                                                                                                   |
| <threshold> | <1-2147483647> Threshold above which to generate a warning message. The mroute warning threshold must not exceed the mroute limit. |

**Default** The default limit and threshold value is 2147483647.

**Mode** Global Configuration

**Usage notes** This command limits the number of multicast IPv4 routes (mroutes) that can be added to a router, and generates an error message when the limit is exceeded. If the threshold parameter is set, a threshold warning message is generated when this threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the limit argument.

**Examples** `awplus# configure terminal`  
`awplus(config)# ip multicast route-limit 34 24`  
`awplus# configure terminal`  
`awplus(config)# no ip multicast route-limit`

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip multicast wrong-vif-suppression

**Overview** Use this command to prevent unwanted multicast packets received on an unexpected interface being trapped to the CPU.

Use the no variant of this command to disable wrong VIF suppression.

**Syntax** `ip ip multicast wrong-vif-suppression`  
`no ip multicast wrong-vif-suppression`

**Default** By default, this feature is disabled.

**Mode** Global Configuration

**Usage notes** Use this command if there is excessive CPU load and multicast traffic is enabled. To confirm that VIF messages are being sent to the CPU use the [debug nsm mcast6](#) command.

**Examples** To enable the suppression of wrong VIF packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast wrong-vif-suppression
```

To disable the suppression of wrong VIF packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast wrong-vif-suppression
```



# ip multicast-routing

**Overview** Use this command to turn on/off IPv4 multicast routing on the router; when turned off the device does not perform multicast functions.

Use the **no** variant of this command to disable IPv4 multicast routing after enabling it. Note the default stated below.

**Syntax** `ip multicast-routing`  
`no ip multicast-routing`

**Default** By default, IPv4 multicast routing is off.

**Mode** Global Configuration

**Usage notes** When the **no** variant of this command is used, the Multicast Routing Information Base (MRIB) cleans up Multicast Routing Tables (MRT), stops IGMP operation, and stops relaying multicast forwarder events to multicast protocols.

When multicast routing is enabled, the MRIB starts processing any MRT addition/deletion requests, and any multicast forwarding events.

You must enable multicast routing before issuing other multicast commands.

**Example** `awplus# configure terminal`  
`awplus(config)# ip multicast-routing`

**Validation  
Commands** `show running-config`

**Command  
changes** Version 5.4.7-1.1: VRF-lite support added for SBx8100.  
Version 5.4.8-1.1: VRF-lite support added for x930, SBx908 GEN2.

# ipv6 mroute

**Overview** Use this command to inform multicast of the RPF (Reverse Path Forwarding) route to a given IPv6 multicast source.

Use the **no** variant of this command to delete a route to an IPv6 multicast source.

**Syntax**

```
ipv6 mroute <ipv6-source-address/mask-length>
[<rpf-interface>] [<rpf-address>] [rip|static]
[<admin-distance>]

no ipv6 mroute <ipv6-source-address/mask-length> [static]
```

| Parameter                         | Description                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv6-source-address/mask-length> | A multicast source IPv6 address and mask length, in hexadecimal notation in the format X.X::X.X/M.                                                                                                                                                                                                                                                  |
| rip                               | RIPng IPv6 unicast routing protocol.                                                                                                                                                                                                                                                                                                                |
| static                            | Specifies a static route.                                                                                                                                                                                                                                                                                                                           |
| <rpf-interface>                   | The RPF interface or the pseudo-interface <b>null</b> .                                                                                                                                                                                                                                                                                             |
| <rpf-address>                     | X.X::X:X<br>The closest known address on the IPv6 multicast route back to the specified source. This host IPv6 address can be within a directly connected subnet or within a remote subnet. In the case that the address is in a remote subnet, a lookup is done from the unicast route table to find the nexthop address on the path to this host. |
| <admin-distance>                  | The administrative distance. Use this to determine whether the RPF lookup selects the unicast or multicast route. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence. The default is 0 and the range available is 0-255.                    |

**Mode** Global Configuration

**Usage notes** Typically, when a Layer 3 multicast routing protocol is determining the RPF (Reverse Path Forwarding) interface for the path to a multicast source, it uses the unicast IPv6 route table to find the best path to the source. However, in some networks a deliberate choice is made to send multicast via different paths to those used for unicast. In this case, the interface via which a multicast stream from a given source enters a router may not be the same as the interface that connects to the best unicast route to that source.

This command enables the user to statically configure the switch with "multicast routes" back to given sources. When performing the RPF check on a stream from a given IPv6 source, the multicast routing protocol will look at these static entries as well as looking into the unicast routing table. The route with the lowest

administrative distance - whether a static “multicast route” or a route from the unicast route table - will be chosen as the RPF route to the source.

Note that in this context the term “multicast route” does not imply a route via which the current router will forward multicast; instead it refers to the route the multicast will have traversed in order to arrive at the current router.

**Examples** The following example creates a static multicast route back to the sources in the 2001::1/64 subnet. The multicast route is via the host 2002::2, and has an administrative distance of 2:

```
awplus# configure terminal
awplus(config)# ipv6 mroute 2001::1/64 static 2 2002::2
```

The following example creates a static multicast route back to the sources in the 2002::2/64 subnet. The multicast route is via the host 2001::1. The administrative distance on this route has the default value of 0:

```
awplus# configure terminal
awplus(config)# ipv6 mroute 2002::2/64 2001::1
```

**Validation  
Commands**

- clear ipv6 mroute
- show ipv6 mroute
- show ipv6 mroute

# ipv6 multicast route

**Overview** Use this command to add an IPv6 static multicast route for a specific multicast source and group IPv6 address to the multicast Routing Information Base (RIB). This IPv6 multicast route is used to forward IPv6 multicast traffic from a specific source and group ingressing on an upstream interface to a single or range of downstream interfaces.

Use the **no** variant of this command to either remove an IPv6 static multicast route set with this command or to remove a specific downstream interface from an IPv6 static multicast route for a specific IPv6 multicast source and group address.

**Syntax** `ipv6 multicast route <ipv6-source-addr> <ipv6-group-addr> <upstream-interface> [<downstream-interface>]`  
`no ipv6 multicast route <ipv6-source-addr> <ipv6-group-addr> [<upstream-interface> <downstream-interface>]`

| Parameter                                 | Description                                                                          |
|-------------------------------------------|--------------------------------------------------------------------------------------|
| <code>&lt;ipv6-source-addr&gt;</code>     | Source IPv6 address, in dotted decimal notation in the format X.X::X.X.              |
| <code>&lt;ipv6-group-addr&gt;</code>      | Group IP address, in dotted decimal notation in the format X.X::X.X.                 |
| <code>&lt;upstream-interface&gt;</code>   | Upstream interface on which the multicast packets ingress.                           |
| <code>&lt;downstream-interface&gt;</code> | Downstream interface or range of interfaces to which the multicast packets are sent. |

**Default** By default, no static routes exist.

**Mode** Global Configuration

**Usage notes** Only one multicast route entry per IPv6 address and multicast group can be specified. Therefore, if one entry for an IPv6 static multicast route is configured, PIM will not be able to update this multicast route in any way.

If a dynamic multicast route exists, you cannot create a static multicast route with the same source IPv6 address and group IPv6 address. An error message is displayed and logged. To add a new static multicast route, either wait for the dynamic multicast route to time out or clear the dynamic multicast route with the [clear ipv6 mroute](#) command.

To update an existing IPv6 static multicast route entry with new or additional downstream interfaces, you must first remove the existing static multicast route and then add the new static multicast route with all downstream interfaces specified. If you attempt to update an existing static multicast route entry with an additional interface or interfaces an error message is displayed and logged.

To remove a specific downstream interface from an existing static multicast route entry, specify the interface you want to remove with the *<downstream-interface>* parameter when entering the **no** variant of this command.

**Examples** To create an IPv6 static multicast route for the multicast source IPv6 address 2001::1 and group IPv6 address ff08::1, specifying the upstream interface as eth0 and the downstream interface as eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast route 2001::1 ff08::1 eth0 eth1
```

To create a blackhole route for the IPv6 multicast source IP address 2001::1 and group IP address ff08::1, specifying the upstream interface as eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast route 2001::1 ff08::1 eth0
```

To delete an IPv6 static multicast route for the multicast source IPv6 address 2001::1 and group IPv6 address ff08::1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 multicast route 2001::1 ff08::1
```

**Related commands** [clear ipv6 mroute](#)

# ipv6 multicast route-limit

**Overview** Use this command to limit the number of multicast routes that can be added to an IPv6 multicast routing table.

Use the **no** variant of this command to return the IPv6 route limit to the default.

**Syntax** `ipv6 multicast route-limit <limit> [<threshold>]`  
`no ipv6 multicast route-limit`

| Parameter   | Description                                                                                                                        |
|-------------|------------------------------------------------------------------------------------------------------------------------------------|
| <limit>     | <1-2147483647> Number of routes.                                                                                                   |
| <threshold> | <1-2147483647> Threshold above which to generate a warning message. The mroute warning threshold must not exceed the mroute limit. |

**Default** The default limit and threshold value is 2147483647.

**Mode** Global Configuration

**Usage notes** This command limits the number of multicast IPv6 routes (mroutes) that can be added to a router, and generates an error message when the limit is exceeded. If the threshold parameter is set, a threshold warning message is generated when this threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the limit argument.

**Examples** To change the limit to 34 routes and the warning threshold to 24 routes, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast route-limit 34 24
```

To return to the default limits, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 multicast route-limit
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 multicast-routing

**Overview** Use this command to turn on/off IPv6 multicast routing on the router; when turned off the device does not perform multicast functions.

Use the **no** variant of this command to disable IPv6 multicast routing after enabling it. Note the default stated below.

**Syntax** `ipv6 multicast-routing`  
`no ipv6 multicast-routing`

**Default** Off

**Mode** Global Configuration

**Usage** When the **no** variant of this command is used, the Multicast Routing Information Base (MRIB) cleans up Multicast Routing Tables (MRT), and stops relaying multicast forwarder events to multicast protocols.

When multicast routing is enabled, the MRIB starts processing any MRT addition/deletion requests, and any multicast forwarding events.

You must enable multicast routing before issuing other multicast commands.

**Examples** To enable multicast routing, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast-routing
```

To disable multicast routing again, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 multicast-routing
```

**Validation  
Commands** [show running-config](#)

**Command  
changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show debugging nsm mcast

**Overview** Use this command to show the status of the NSM multicast debugging.

**Syntax** `show debugging nsm mcast`

**Mode** Privileged Exec

**Usage notes** This command is intended for use by Allied Telesis authorized service personnel for diagnostic purposes.

**Example** To show debugging for NSM multicast, use the following command:

```
awplus# show debug nsm mcast
```

**Output** Figure 30-1: Example output from **show debug nsm mcast**

```
awplus# show debugging nsm mcast
Debugging status:
 NSM multicast vif debugging is on
 NSM multicast route debugging is on
 NSM multicast route statistics debugging is on
 NSM multicast FIB message debugging is on
 NSM multicast PIM Register message debugging is on
 NSM multicast traceroute debugging is on
 NSM multicast traceroute detailed debugging is on
```

**Related commands** [debug nsm mcast](#)

**Command changes** Version 5.4.7-2.1: command added  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2



# show ip mroute

**Overview** Use this command to display the contents of the IPv4 multicast routing (mroute) table.

**Syntax** `show ip mroute [<ipv4-group-addr>] [<ipv4-source-addr>]  
[dense|sparse|static] [count|summary]`

| Parameter          | Description                                                                               |
|--------------------|-------------------------------------------------------------------------------------------|
| <ipv4-group-addr>  | Group IPv4 address, in dotted decimal notation in the format A.B.C.D.                     |
| <ipv4-source-addr> | Source IPv4 address, in dotted decimal notation in the format A.B.C.D.                    |
| dense              | Display dense IPv4 multicast routes.                                                      |
| sparse             | Display sparse IPv4 multicast routes.                                                     |
| static             | Display static IPv4 multicast routes.                                                     |
| count              | Display the route and packet count from the IPv4 multicast routing (mroute) table.        |
| summary            | Display the contents of the IPv4 multicast routing (mroute) table in an abbreviated form. |

**Mode** User Exec and Privileged Exec

**Examples**

```
awplus# show ip mroute 10.10.3.34 224.1.4.3
awplus# show ip mroute 10.10.5.24 225.2.2.2 count
awplus# show ip mroute 10.10.1.34 summary
```

**Output** The following is a sample output of this command displaying the IPv4 multicast routing table, with and without specifying the group and source IPv4 address:

Figure 30-2: Example output from the **show ip mroute** command

```
awplus# show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SM, Flags: TF
 Incoming interface: eth0
 Outgoing interface list:
 eth1 (1)
```

Figure 30-3: Example output from the **show ip mroute** command with the source and group IPv4 address specified

```
awplus# show ip mroute 10.10.1.52 224.0.1.3

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), uptime 00:03:24, stat expires 00:01:28
Owner PIM-SM, Flags: TF
 Incoming interface: eth0
 Outgoing interface list:
 eth1 (1)
```

The following is a sample output of this command displaying the packet count from the IPv4 multicast routing table:

Figure 30-4: Example output from the **show ip mroute count** command

```
awplus# show ip mroute count
IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT rcv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK rcv/Reg NACK rcv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If
pkts
Fwd msg counts: WRONGVIF/WHOLEPKT rcv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK rcv/Reg NACK rcv/Reg pkt sent

(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
 Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following is a sample output for this command displaying the IPv4 multicast routing table in an abbreviated form:

Figure 30-5: Example output from the **show ip mroute summary** command

```
awplus# show ip mroute summary

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM, Flags: TF
```

**Command  
changes**

Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# show ip mvif

**Overview** Use this command to display the contents of the IPv4 Multicast Routing Information Base (MRIB) VIF table.

**Syntax** `show ip mvif <interface>`

| Parameter   | Description                                 |
|-------------|---------------------------------------------|
| <interface> | The interface to display information about. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip mvif eth0`

**Output** Figure 30-6: Example output from the **show ip mvif** command

| Interface | Vif<br>Idx | Owner<br>Module | TTL | Local<br>Address | Remote<br>Address | Uptime   |
|-----------|------------|-----------------|-----|------------------|-------------------|----------|
| eth0      | 0          | PIM-SM          | 1   | 192.168.1.53     | 0.0.0.0           | 00:04:26 |
| Register  | 1          |                 | 1   | 192.168.1.53     | 0.0.0.0           | 00:04:26 |
| eth1      | 2          | PIM-SM          | 1   | 192.168.10.53    | 0.0.0.0           | 00:04:25 |

**Command changes** Version 5.4.7-1.1: VRF-lite support added for SBx8100.  
Version 5.4.8-1.1: VRF-lite support added for x930, SBx908 GEN2.

# show ip rpf

**Overview** Use this command to display Reverse Path Forwarding (RPF) information for the specified IPv4 source address.

**Syntax** `show ip rpf <source-addr>`

| Parameter                        | Description                                                            |
|----------------------------------|------------------------------------------------------------------------|
| <code>&lt;source-addr&gt;</code> | Source IPv4 address, in dotted decimal notation in the format A.B.C.D. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip rpf 10.10.10.50`

**Command changes** Version 5.4.7-1.1: VRF-lite support added for SBx8100.  
Version 5.4.8-1.1: VRF-lite support added for x930, SBx908 GEN2.

# show ipv6 mif

**Overview** Use this command to display the contents of the IPv6 Multicast Routing Information Base (MRIB) MIF table.

**Syntax** `show ipv6 mif [<interface>]`

| Parameter   | Description                                |
|-------------|--------------------------------------------|
| <interface> | An interface to display information about. |

**Mode** User Exec and Privileged Exec

**Example** To display the contents of the MIF table for all interfaces, use the following command:

```
awplus# show ipv6 mif
```

To display the contents of the MIF table for a specific interface, use the following command:

```
awplus# show ipv6 mif eth0
```

**Output** Figure 30-7: Example output from the **show ipv6 mif** command

```
awplus#show ipv6 mif
```

| Interface | Mif | Owner                 | Uptime   |
|-----------|-----|-----------------------|----------|
|           | Idx | Module                |          |
| eth1      | 0   | MLD/MLD Proxy-Service | 03:28:48 |
| eth0      | 1   | MLD/MLD Proxy-Service | 03:28:48 |

Figure 30-8: Example output from the **show ipv6 mif** command with the interface parameter specified

| Interface | Mif | Owner                 | TTL | Remote  | Uptime   |
|-----------|-----|-----------------------|-----|---------|----------|
|           | Idx | Module                |     | Address |          |
| eth0      | 0   | MLD/MLD Proxy-Service | 1   | 0.0.0.0 | 00:05:17 |

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 mroute

**Overview** Use this command to display the contents of the IPv6 multicast routing (mroute) table.

**Syntax** `show ipv6 mroute [<ipv6-group-addr>] [<ipv6-source-addr>]  
[{count|summary}]`

| Parameter          | Description                                                                               |
|--------------------|-------------------------------------------------------------------------------------------|
| <ipv6-group-addr>  | Group IPv6 address, in hexadecimal notation in the format X.X::X.X.                       |
| <ipv6-source-addr> | Source IPv6 address, in hexadecimal notation in the format X.X::X.X.                      |
| count              | Display the route and packet count from the IPv6 multicast routing (mroute) table.        |
| summary            | Display the contents of the IPv6 multicast routing (mroute) table in an abbreviated form. |

**Mode** User Exec and Privileged Exec

**Examples**

```
awplus# show ipv6 mroute
awplus# show ipv6 mroute count
awplus# show ipv6 mroute summary
awplus# show ipv6 mroute 2001::2 ff08::1 count
awplus# show ipv6 mroute 2001::2 ff08::1
awplus# show ipv6 mroute 2001::2 summary
```

**Output** The following is a sample output of this command displaying the IPv6 multicast routing table for a single static IPv6 Multicast route:

Figure 30-9: Example output from the **show ipv6 mroute** command

```
awplus#show ipv6 mroute
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface
(2001::2, ff08::1), uptime 03:18:38
Owner IMI, Flags: F
Incoming interface: eth0
Outgoing interface list:
eth1
```

The following is a sample output of this command displaying the IPv6 multicast routing count table for a single static IPv6 Multicast route:

Figure 30-10: Example output from the **show ipv6 mroute count** command

```
awplus#show ipv6 mroute count

IPv6 Multicast Statistics
Total 1 routes using 152 bytes memory
Route limit/Route threshold: 1024/1024
Total NOCACHE/WRONGmif/WHOLEPKT rcv from fwd: 6/0/0
Total NOCACHE/WRONGmif/WHOLEPKT sent to clients: 6/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK rcv/Reg NACK rcv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:14

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If
pkts
Fwd msg counts: WRONGmif/WHOLEPKT rcv
Client msg counts: WRONGmif/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK rcv/Reg NACK rcv/Reg pkt sent

(2001::2, ff08::1), Forwarding: 0/0, Other: 0
 Fwd msg: 0/0, Client msg: 0/0/0/0, Reg: 0/0/0
```

The following is a sample output of this command displaying the IPv6 multicast routing summary table for a single static IPv6 Multicast route:

Figure 30-11: Example output from the **show ipv6 mroute summary** command

```
awplus#show ipv6 mroute summary

IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface

(2001::2, ff08::1), 03:20:28/-, IMI, Flags: F
```



# show ipv6 multicast forwarding

**Overview** Use this command to view the status of multicast forwarding.

**Syntax** `show ipv6 multicast forwarding`

**Mode** Privileged Exec

**Example** To show the status of the multicast forwarding, use the following command:

```
awplus# show ipv6 multicast forwarding
```

**Output** Figure 30-12: Example output from the **show ipv6 multicast forwarding** command:

```
ipv6 multicast forwarding is disabled
```

**Related commands** [ipv6 multicast forward-slow-path-packet](#)

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# 31

# PIM-SM Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of PIM-SM commands. For commands common to PIM-SM and PIM-DM, see the [Multicast Commands](#) chapter.

- Command List**
- “clear ip pim sparse-mode bsr rp-set \*” on page 1416
  - “clear ip pim sparse-mode packet statistics” on page 1417
  - “clear ip mroute pim sparse-mode” on page 1418
  - “debug pim sparse-mode” on page 1419
  - “debug pim sparse-mode timer” on page 1420
  - “ip pim anycast-rp” on page 1422
  - “ip pim bsr-border” on page 1423
  - “ip pim bsr-candidate” on page 1424
  - “ip pim cisco-register-checksum” on page 1425
  - “ip pim crp-cisco-prefix” on page 1426
  - “ip pim dr-priority” on page 1427
  - “ip pim exclude-genid” on page 1428
  - “ip pim ext-srcs-directly-connected” on page 1429
  - “ip pim hello-holdtime (PIM-SM)” on page 1430
  - “ip pim hello-interval (PIM-SM)” on page 1431
  - “ip pim ignore-rp-set-priority” on page 1432
  - “ip pim jp-timer” on page 1433
  - “ip pim register-rate-limit” on page 1434
  - “ip pim register-rp-reachability” on page 1435

- [“ip pim register-source”](#) on page 1436
- [“ip pim register-suppression”](#) on page 1437
- [“ip pim rp-address”](#) on page 1438
- [“ip pim rp-candidate”](#) on page 1440
- [“ip pim rp-register-kat”](#) on page 1441
- [“ip pim sparse-mode”](#) on page 1442
- [“ip pim sparse-mode join-prune-batching”](#) on page 1443
- [“ip pim sparse-mode passive”](#) on page 1444
- [“ip pim sparse-mode wrong-vif-suppression”](#) on page 1445
- [“ip pim spt-threshold”](#) on page 1446
- [“ip pim ssm”](#) on page 1447
- [“service pim”](#) on page 1448
- [“show debugging pim sparse-mode”](#) on page 1449
- [“show ip pim sparse-mode bsr-router”](#) on page 1450
- [“show ip pim sparse-mode interface”](#) on page 1451
- [“show ip pim sparse-mode interface detail”](#) on page 1453
- [“show ip pim sparse-mode local-members”](#) on page 1454
- [“show ip pim sparse-mode mroute”](#) on page 1455
- [“show ip pim sparse-mode mroute detail”](#) on page 1457
- [“show ip pim sparse-mode neighbor”](#) on page 1459
- [“show ip pim sparse-mode nexthop”](#) on page 1461
- [“show ip pim sparse-mode packet statistics”](#) on page 1462
- [“show ip pim sparse-mode rp-hash”](#) on page 1463
- [“show ip pim sparse-mode rp mapping”](#) on page 1464
- [“undebg all pim sparse-mode”](#) on page 1465

# clear ip pim sparse-mode bsr rp-set \*

**Overview** Use this command to clear all Rendezvous Point (RP) sets learned through the PIMv2 Bootstrap Router (BSR).

**Syntax** `clear ip pim sparse-mode bsr rp-set *`

| Parameter | Description         |
|-----------|---------------------|
| *         | Clears all RP sets. |

**Mode** Privileged Exec

**Usage notes** For multicast clients, note that one router will be automatically or statically designated as the RP, and all routers must explicitly join through the RP. A Designated Router (DR) sends periodic Join/Prune messages toward a group-specific RP for each group that it has active members.

For multicast sources, note that the Designated Router (DR) unicasts Register messages to the RP encapsulating the data packets from the multicast source. The RP forwards decapsulated data packets toward group members.

**Example** `awplus# clear ip pim sparse-mode bsr rp-set *`

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# clear ip pim sparse-mode packet statistics

**Overview** Use this command to clear the PIM sparse mode packet statistics counter.

**Syntax** `clear ip pim sparse-mode packet statistics`

**Mode** Privileged Exec

**Example** The following command clears the current packet receive counts for PIM sparse-mode:

```
awplus# configure terminal
awplus(config)# clear ip pim sparse-mode statistics
```

**Output** Figure 31-1: Example output from **clear ip pim sparse-mode statistics**

```
awplus(config)#clear ip pim sparse-mode statistics
PIM-SM Receive Packet Statistics :
All PIM-SM : Total : 0 Valid : 0
Hello : Total : 0 Valid : 0
Register : Total : 0 Valid : 0
Register Stop : Total : 0 Valid : 0
Join/Prune : Total : 0 Valid : 0
Bootstrap : Total : 0 Valid : 0
Assert : Total : 0 Valid : 0
Candidate-RP : Total : 0 Valid : 0
```

**Related commands** [show ip pim sparse-mode packet statistics](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# clear ip mroute pim sparse-mode

**Overview** Use this command to clear all multicast route table entries learned through PIM-SM for a specified multicast group address, and optionally a specified multicast source address.

**Syntax** `clear ip mroute <Group-IP-address> pim sparse-mode`  
`clear ip mroute <Group-IP-address> <Source-IP-address> pim sparse-mode`

| Parameter                              | Description                                                          |
|----------------------------------------|----------------------------------------------------------------------|
| <code>&lt;Group-IP-address&gt;</code>  | Specify a multicast group IPv6 address, entered in the form A.B.C.D. |
| <code>&lt;Source-IP-address&gt;</code> | Specify a source group IP address, entered in the form A.B.C.D.      |

**Mode** Privileged Exec

**Example** `awplus# clear ip mroute pim sparse-mode 224.0.0.0`  
`awplus# clear ip mroute 192.168.7.1 pim sparse-mode 224.0.0.0`

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# debug pim sparse-mode

**Overview** Use this command to turn on some or all PIM-SM debugging.

Use the **no** variant of this command to turn off some or all PIM-SM debugging.

**Syntax** `debug pim sparse-mode [all] [events] [mfc] [mib] [nexthop] [nsm] [packet] [state] [mtrace]`  
`no debug pim sparse-mode [all] [events] [mfc] [mib] [nexthop] [nsm] [packet] [state] [mtrace]`

| Parameter | Description                                                                                |
|-----------|--------------------------------------------------------------------------------------------|
| all       | Activates/deactivates all PIM-SM debugging.                                                |
| events    | Activates debug printing of events.                                                        |
| mfc       | Activates debug printing of MFC (Multicast Forwarding Cache in kernel) add/delete/updates. |
| mib       | Activates debug printing of PIM-SM MIBs.                                                   |
| nexthop   | Activates debug printing of PIM-SM next hop communications.                                |
| nsm       | Activates debugging of PIM-SM Network Services Module communications.                      |
| packet    | Activates debug printing of incoming and/or outgoing packets.                              |
| state     | Activates debug printing of state transition on all PIM-SM FSMs.                           |
| mtrace    | Activates debug printing of multicast traceroute.                                          |

**Mode** Privileged Exec and Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# debug pim sparse-mode all`

**Related commands** [show debugging pim sparse-mode](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# debug pim sparse-mode timer

**Overview** Use this command to enable debugging for the specified PIM-SM timers.

Use the **no** variants of this command to disable debugging for the specified PIM-SM timers.

**Syntax**

```
debug pim sparse-mode timer assert [at]
no debug pim sparse-mode timer assert [at]
debug pim sparse-mode timer bsr [bst|crp]
no debug pim sparse-mode timer bsr [bst|crp]
debug pim sparse-mode timer hello [ht|nlt|tht]
no debug pim sparse-mode timer hello [ht|nlt|tht]
debug pim sparse-mode timer joinprune [jt|et|ppt|kat|ot]
no debug pim sparse-mode timer joinprune [jt|et|ppt|kat|ot]
debug pim sparse-mode timer register [rst]
no debug pim sparse-mode timer register [rst]
```

| Parameter | Description                                                                                           |
|-----------|-------------------------------------------------------------------------------------------------------|
| assert    | Enable or disable debugging for the Assert timers.                                                    |
| at        | Enable or disable debugging for the Assert Timer.                                                     |
| bsr       | Enable or disable debugging for the specified Bootstrap Router timer, or all Bootstrap Router timers. |
| bst       | Enable or disable debugging for the Bootstrap Router: Bootstrap Timer.                                |
| crp       | Enable or disable debugging for the Bootstrap Router: Candidate-RP Timer.                             |
| hello     | Enable or disable debugging for the specified Hello timer, or all Hello timers.                       |
| ht        | Enable or disable debugging for the Hello timer: Hello Timer.                                         |
| nlt       | Enable or disable debugging for the Hello timer: Neighbor Liveness Timer.                             |
| tht       | Enable or disable debugging for the Hello timer: Triggered Hello Timer.                               |
| joinprune | Enable or disable debugging for the specified JoinPrune timer, or all JoinPrune timers.               |
| jt        | Enable or disable debugging for the JoinPrune timer: upstream Join Timer.                             |
| et        | Enable or disable debugging for the JoinPrune timer: Expiry Timer.                                    |
| ppt       | Enable or disable debugging for the JoinPrune timer: PrunePending Timer.                              |



| Parameter | Description                                                                   |
|-----------|-------------------------------------------------------------------------------|
| kat       | Enable or disable debugging for the JoinPrune timer: KeepAlive Timer.         |
| ot        | Enable or disable debugging for the JoinPrune timer: Upstream Override Timer. |
| register  | Enable or disable debugging for the Register timers.                          |
| rst       | Enable or disable debugging for the Register timer: Register Stop Timer.      |

**Default** By default, all debugging is disabled.

**Mode** Privileged Exec and Global Configuration

**Examples** To enable debugging for the PIM-SM Bootstrap Router bootstrap timer, use the commands:

```
awplus(config)# debug pim sparse-mode timer bsr bst
```

To enable debugging for the PIM-SM Hello: neighbor liveness timer, use the command:

```
awplus(config)# debug pim sparse-mode timer hello ht
```

To enable debugging for the PIM-SM Joinprune expiry timer, use the command:

```
awplus# debug pim sparse-mode timer joinprune et
```

To disable debugging for the PIM-SM Register timer, use the command:

```
awplus# no debug pim sparse-mode timer register
```

**Related commands** [show debugging pim sparse-mode](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim anycast-rp

**Overview** Use this command to configure Anycast RP (Rendezvous Point) in a RP set.

Use the **no** variant of this command to remove the configuration.

**Syntax** `ip pim anycast-rp <anycast-rp-address> <member-rp-address>`  
`no ip pim anycast-rp <anycast-rp-address> [<member-rp-address>]`

| Parameter                               | Description                                                                                        |
|-----------------------------------------|----------------------------------------------------------------------------------------------------|
| <code>&lt;anycast-rp-address&gt;</code> | <A.B.C.D> Specify an anycast IP address to configure an Anycast RP (Rendezvous Point) in a RP set. |
| <code>&lt;member-rp-address&gt;</code>  | <A.B.C.D> Specify an Anycast RP (Rendezvous Point) address to configure an Anycast RP in a RP set. |

**Mode** Global Configuration

**Usage notes** Anycast is a network addressing and routing scheme where data is routed to the nearest or best destination as viewed by the routing topology. Compared to unicast with a one-to-one association between network address and network endpoint, and multicast with a one-to-many association between network address and network endpoint; anycast has a one-to-many association between network address and network endpoint. For anycast, each destination address identifies a set of receiver endpoints, from which only one receiver endpoint is chosen.

Anycast is often implemented using BGP to simultaneously advertise the same destination IP address range from many sources, resulting in packets address to destination addresses in this range being routed to the nearest source announcing the given destination IP address.

Use this command to specify the Anycast RP configuration in the Anycast RP set. Use the **no** variant of this command to remove the Anycast RP configuration. Note that the member RP address is optional when using the **no** parameter to remove the Anycast RP configuration. removing the anycast RP address also removes the member RP address.

**Examples** The following example shows how to configure the Anycast RP address with **ip pim anycast-rp**:

```
awplus# configure terminal
awplus(config)# ip pim anycast-rp 1.1.1.1 10.10.10.10
```

The following example shows how to remove the Anycast RP in the RP set specifying only the anycast RP address with **no ip pim anycast-rp**, but not specifying the member RP address:

```
awplus# configure terminal
awplus(config)# no ip pim anycast-rp 1.1.1.1
```

# ip pim bsr-border

**Overview** Use the **ip pim bsr-border** command to prevent Bootstrap Router (BSR) messages from being sent or received through an interface. The BSR border is the border of the PIM domain.

Use the **no** variant of this command to disable the configuration set with **ip pim bsr-border**.

**Syntax** `ip pim bsr-border`  
`no ip pim bsr-border`

**Mode** Interface Configuration for an Eth or PPP interface.

**Usage notes** When this command is configured on an interface, no PIM version 2 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two PIM domains.

BSR messages should not be exchanged between different domains, because devices in one domain may elect Rendezvous Points (RPs) in the other domain, resulting in loss of isolation between the two PIM domains that would stop the PIM protocol from working as intended.

**Examples** The following example configures the eth1 interface to be the PIM domain border:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip pim bsr-border
```

The following example removes the eth1 interface from the PIM domain border:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip pim bsr-border
```

The following example configures the PPP interface ppp0 to be the PIM domain border:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip pim bsr-border
```

The following example removes the PPP interface ppp0 from the PIM domain border:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip pim bsr-border
```

# ip pim bsr-candidate

**Overview** Use this command to give the device the candidate BSR (Bootstrap Router) status using the specified IP address mask of the interface.

Use the **no** variant of this command to withdraw the address of the interface from being offered as a BSR candidate.

**Syntax** `ip pim bsr-candidate <interface> [<hash>] [<priority>]`  
`no ip pim bsr-candidate [<interface>]`

| Parameter   | Description                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface> | The interface.                                                                                                                                                                                              |
| <hash>      | <0-32> configure hash mask length for RP selection. The default hash value if you do not configure this parameter is 10.                                                                                    |
| <priority>  | <0-255> configure priority for a BSR candidate. Note that you must also specify the <hash> (mask length) when specifying the <priority>. The default priority if you do not configure this parameter is 64. |

**Mode** Global Configuration

**Default** The default hash parameter value is 10 and the default priority parameter value is 64.

**Examples** To set the BSR candidate to the eth1 interface, with the optional mask length and BSR priority parameters, enter the commands shown below:

```
awplus# configure terminal
awplus(config)# ip pim bsr-candidate eth1 20 30
```

To withdraw the address of eth1 from being offered as a BSR candidate, enter:

```
awplus# configure terminal
awplus(config)# no ip pim bsr-candidate eth1
```

To set the BSR candidate to the PPP interface ppp0, with the optional mask length and BSR priority parameters, enter the commands shown below:

```
awplus# configure terminal
awplus(config)# ip pim bsr-candidate ppp0 20 30
```

To withdraw the address of ppp0 from being offered as a BSR candidate, enter:

```
awplus# configure terminal
awplus(config)# no ip pim bsr-candidate ppp0
```

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim cisco-register-checksum

**Overview** Use this command to configure the option to calculate the Register checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to disable this option.

**Syntax** `ip pim cisco-register-checksum`  
`no ip pim cisco-register-checksum`

**Default** This command is disabled by default. By default, Register Checksum is calculated only over the header.

**Mode** Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# ip pim cisco-register-checksum`

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim crp-cisco-prefix

**Overview** Use this command to interoperate with Cisco devices that conform to an earlier draft standard. Some Cisco devices might not accept candidate RPs with a group prefix number of zero. Note that the latest BSR specification prohibits sending RP advertisements with prefix 0. RP advertisements for the default IPv4 multicast group range 224/4 are sent with a prefix of 1.

Use the **no** variant of this command to revert to the default settings.

**Syntax** `ip pim crp-cisco-prefix`  
`no ip pim crp-cisco-prefix`

**Mode** Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# ip pim crp-cisco-prefix`  
`awplus# configure terminal`  
`awplus(config)# no ip pim crp-cisco-prefix`

**Related commands** [ip pim rp-candidate](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim dr-priority

**Overview** Use this command to set the Designated Router priority value.  
Use the **no** variant of this command to disable this function.

**Syntax** `ip pim dr-priority <priority>`  
`no ip pim dr-priority [<priority>]`

| Parameter  | Description                                                                                                                                      |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <priority> | Specify the Designated Router priority value, in the range 0 to 4294967294. Note that a higher value has a higher preference or higher priority. |

**Default** The default is 1. The negated form of this command restores the value to the default.

**Mode** Interface Configuration for a Eth or a PPP interface.

**Examples** To set the Designated Router priority value to 11234 for the eth1 interface, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip pim dr-priority 11234
```

To disable the Designated Router priority value for the eth1 interface, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip pim dr-priority
```

To set the Designated Router priority value to 11234 for the PPP interface ppp0, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip pim dr-priority 11234
```

To disable the Designated Router priority value for the PPP interface ppp0, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip pim dr-priority
```

**Related commands** [ip pim ignore-rp-set-priority](#)

# ip pim exclude-genid

**Overview** Use this command to exclude the GenID option from Hello packets sent out by the PIM module on a particular interface. This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to revert to default settings.

**Syntax** `ip pim exclude-genid`  
`no ip pim exclude-genid`

**Default** By default, this command is disabled; the GenID option is included.

**Mode** Interface Configuration for a Eth or a PPP interface.

**Example** To exclude the GenID option on interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip pim exclude-genid
```

To exclude the GenID option on interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip pim exclude-genid
```



# ip pim ext-srcs-directly-connected

**Overview** Use this command to configure PIM to treat all source traffic arriving on the interface as though it was sent from a host directly connected to the interface.

Use the **no** variant of this command to configure PIM to treat only directly connected sources as directly connected.

**Syntax** `ip pim ext-srcs-directly-connected`  
`no ip pim ext-srcs-directly-connected`

**Default** The **no** variant of this command is the default behavior.

**Mode** Interface Configuration for a Eth or a PPP interface.

**Example** To configure PIM to treat all sources as directly connected for eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip pim ext-srcs-directly-connected
```

To configure PIM to treat only directly connected sources as directly connected for eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip pim ext-srcs-directly-connected
```

To configure PIM to treat all sources as directly connected for PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip pim ext-srcs-directly-connected
```

To configure PIM to treat only directly connected sources as directly connected for PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip pim ext-srcs-directly-connected
```

# ip pim hello-holdtime (PIM-SM)

**Overview** This command configures a hello-holdtime value. You cannot configure a hello-holdtime value that is less than the current hello-interval.

Use the **no** variant of this command to return it to its default of 3.5 \* the current hello-interval.

**Syntax** `ip pim hello-holdtime <holdtime>`  
`no ip pim hello-holdtime`

| Parameter  | Description                                                                      |
|------------|----------------------------------------------------------------------------------|
| <holdtime> | <1-65535><br>The holdtime value in seconds (no fractional seconds are accepted). |

**Default** The default hello-holdtime value is 3.5 \* the current hello-interval.

**Mode** Interface Configuration for a Eth or a PPP interface.

**Usage** Each time the hello-interval is updated, the hello-holdtime is also updated, according to the following rules:

If the hello-holdtime is not configured; or if the hello-holdtime is configured and less than the current hello-interval value, it is modified to the (3.5 \* hello-interval). Otherwise, it retains the configured value.

**Example** To set the hello-hold time value on interface eth0, use the commands

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip pim hello-holdtime 123
```

To set the hello-hold time value on interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip pim hello-holdtime 123
```

# ip pim hello-interval (PIM-SM)

**Overview** This command configures a hello-interval value.  
Use the **no** variant of this command to reset the hello-interval to the default.

**Syntax** `ip pim hello-interval <interval>`  
`no ip pim hello-interval`

| Parameter  | Description                                                      |
|------------|------------------------------------------------------------------|
| <interval> | <1-65535> The value in seconds (no fractional seconds accepted). |

**Default** The default hello-interval value is 30 seconds.

**Mode** Interface Configuration for a Eth or a PPP interface.

**Usage** When the hello-interval is configured, and the hello-holdtime is not configured, or when the configured hello-holdtime value is less than the new hello-interval value; the holdtime value is modified to the (3.5 \* hello-interval). Otherwise, the hello-holdtime value is the configured value.

**Example** To set the hello-interval value on interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip pim hello-interval 123
```

To set the hello-interval value on interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip pim hello-interval 123
```

# ip pim ignore-rp-set-priority

**Overview** Use this command to ignore the RP-SET priority value, and use only the hashing mechanism for RP selection.

This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to disable this setting.

**Syntax** `ip pim ignore-rp-set-priority`  
`no ip pim ignore-rp-set-priority`

**Mode** Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# ip pim ignore-rp-set-priority`

# ip pim jp-timer

**Overview** Use this command to set the PIM-SM join/prune timer. Note that the value the device puts into the holdtime field of the join/prune packets it sends to its neighbors is 3.5 times the join/prune timer value set using this command.

Use the **no** variant of this command to return the PIM-SM join/prune timer to its default value of 60 seconds, which corresponds to a join/prune packet holdtime of 210 seconds.

**Syntax** `ip pim jp-timer <1-65535>`  
`no ip pim jp-timer [<1-65535>]`

| Parameter | Description                                                            |
|-----------|------------------------------------------------------------------------|
| <1-65535> | Specifies the join/prune timer value. The default value is 60 seconds. |

**Default** The default join/prune timer value is 60 seconds.

**Mode** Global Configuration

**Example** To set the join/prune timer value to 300 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip pim jp-timer 300
```

To return the join/prune timer to its default value of 60 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip pim jp-timer
```

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim register-rate-limit

**Overview** Use this command to configure the rate of register packets sent by this DR, in units of packets per second.

Use the **no** variant of this command to remove the limit.

**Syntax** `ip pim register-rate-limit <1-65535>`  
`no ip pim register-rate-limit`

| Parameter                    | Description                                                          |
|------------------------------|----------------------------------------------------------------------|
| <code>&lt;1-65535&gt;</code> | Specifies the maximum number of packets that can be sent per second. |

**Mode** Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# ip pim register-rate-limit 3444`

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim register-rp-reachability

**Overview** Use this command to enable the RP reachability check for PIM Register processing at the DR. The default setting is no checking for RP-reachability.

Use the **no** variant of this command to disable this processing.

**Syntax** `ip pim register-rp-reachability`  
`no ip pim register-rp-reachability`

**Default** This command is disabled; by default, there is no checking for RP-reachability.

**Mode** Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# ip pim register-rp-reachability`

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim register-source

**Overview** Use this command to configure the source address of register packets sent by this DR, overriding the default source address, which is the address of the RPF interface toward the source host.

Use the **no** variant of this command to un-configure the source address of Register packets sent by this DR, reverting back to use the default source address that is the address of the RPF interface toward the source host.

**Syntax** `ip pim register-source [<source-address>|<interface>]`  
`no ip pim register-source`

| Parameter                           | Description                                                                                    |
|-------------------------------------|------------------------------------------------------------------------------------------------|
| <code>&lt;source-address&gt;</code> | The IP address, entered in the form A.B.C.D, to be used as the source of the register packets. |
| <code>&lt;interface&gt;</code>      | The name of the interface to be used as the source of the register packets.                    |

**Usage notes** The configured address must be a reachable address to be used by the RP to send corresponding Register-Stop messages in response. It is normally the local loopback interface address, but can also be a physical address. This address must be advertised by unicast routing protocols on the DR. The configured interface does not have to be PIM enabled.

**Mode** Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# ip pim register-source 10.10.1.3`

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.



# ip pim register-suppression

**Overview** Use this command to configure the register-suppression time, in seconds, overriding the default of 60 seconds. Configuring this value modifies register-suppression time at the DR. Configuring this value at the RP modifies the RP-keepalive-period value if the [ip pim rp-register-kat](#) command is not used.

Use the **no** variant of this command to reset the value to its default of 60 seconds.

**Syntax** `ip pim register-suppression <1-65535>`  
`no ip pim register-suppression`

**Mode** Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# ip pim register-suppression 192`

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim rp-address

**Overview** Use this command to statically configure the RP (Rendezvous Point) address for multicast groups.

Use the **no** variant of this command to remove a statically configured RP address for multicast groups.

**Syntax** `ip pim rp-address <ip-address> group-list <group-prefix> [override]`  
`no ip pim rp-address <ip-address> group-list <group-prefix> [override]`

| Parameter      | Description                                                            |
|----------------|------------------------------------------------------------------------|
| <ip-address>   | IP address of RP, entered in the form A.B.C.D.                         |
| <group-prefix> | Multicast group IP prefix address of RP, entered in the form A.B.C.D/M |
| override       | Enables statically defined RPs to override dynamically learned RPs.    |

**Mode** Global Configuration

**Usage notes** The AlliedWare Plus PIM-SM implementation supports multiple static RPs. It also supports usage of static RP and the BSR (Bootstrap Router) mechanism simultaneously. The **ip pim rp-address** command is used to statically configure the RP address for multicast groups.

You need to understand the following information before using this command.

If the RP address configured by the BSR, and the statically configured RP address are both available for a group range, then the RP address configured through the BSR is chosen over the statically configured RP address, unless the 'override' parameter is specified, in which case, the static RP will be chosen.

After configuration, the RP address is inserted into a static RP group tree based on the configured group ranges. For each group range, multiple static RPs are maintained in a linked list. This list is sorted in a descending order of IP addresses. When selecting static RPs for a group range, the first element (which is the static RP with highest IP address) is chosen.

RP address deletion is handled by removing the static RP from all the existing group ranges and recalculating the RPs for existing TIB states if required.

**NOTE:** A unique RP address may only be specified once as a static RP.

**Example** `awplus# configure terminal`  
`awplus(config)# ip pim rp-address 192.0.2.10 group-list`  
`233.252.0.0/24 override`

Figure 31-2: Output from the **show ip pim sparse-mode rp mapping** command

```
awplus#show ip pim sp rp mapping
PIM Group-to-RP Mappings
Group(s): 233.252.0.0/24, Static
RP: 192.0.2.10
Uptime: 00:00:17
```

**Related  
commands**

[ip pim rp-candidate](#)  
[ip pim rp-register-kat](#)  
[show ip pim sparse-mode rp mapping](#)

**Command  
changes**

Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-0.5: Replaced <acl> parameter with <group-list> parameter.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim rp-candidate

**Overview** Use this command to make the router an RP (Rendezvous Point) candidate, using the IP address of the specified interface.

Use the **no** variant of this command to remove the RP status set using the **ip pim rp-candidate** command.

**Syntax** `ip pim rp-candidate <interface> [priority <priority>] [interval <interval>]`  
`no ip pim rp-candidate [<interface>]`

| Parameter              | Description                                                                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface>            | Interface name.                                                                                                                                               |
| priority<br><priority> | The RP candidate priority for this interface on this device, from 0 to 255. The lower the priority value, the more likely this candidate is to become the RP. |
| interval<br><interval> | The advertisement interval, from 1 to 16383 seconds.                                                                                                          |

**Default** The priority value for a candidate RP is 192 by default until specified using the **priority** parameter.

**Mode** Global Configuration

**Usage notes** Entering the command **ip pim rp-candidate <interface>** without one of the optional **priority** or **interval** parameters will configure the candidate RP with a priority value of 192.

**Examples** To specify a priority of 3, use the commands:

```
awplus# configure terminal
awplus(config)# ip pim rp-candidate eth1 priority 3
```

To stop the device from being an RP candidate on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# no ip pim rp-candidate eth1
```

**Related commands** [ip pim rp-address](#)  
[ip pim rp-register-kat](#)  
[ip pim crp-cisco-prefix](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim rp-register-kat

**Overview** Use this command to configure the Keep Alive Time (KAT) for (S,G) states at the RP (Rendezvous Point) to monitor PIM-SM Register packets.

Use the **no** variant of this command to return the PIM-SM KAT timer to its default value of 210 seconds.

**Syntax** `ip pim rp-register-kat <1-65535>`  
`no ip pim rp-register-kat`

| Parameter | Description                                                         |
|-----------|---------------------------------------------------------------------|
| <1-65535> | Specify the KAT timer in seconds. The default value is 210 seconds. |

**Mode** Global Configuration

**Default** The default PIM-SM KAT timer value is 210 seconds.

**Examples** `awplus# configure terminal`  
`awplus(config)# ip pim rp-register-kat 3454`  
`awplus# configure terminal`  
`awplus(config)# no ip pim rp-register-kat`

**Related commands** [ip pim rp-address](#)  
[ip pim rp-candidate](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim sparse-mode

**Overview** Use this command to enable PIM-SM on an interface.  
Use the **no** variant of this command to disable PIM-SM on an interface.

**Syntax** `ip pim sparse-mode`  
`no ip pim sparse-mode`

**Mode** Interface Configuration for a Eth or a PPP interface.

**Examples** To enable PIM-SM on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip pim sparse-mode
```

To disable PIM-SM on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip pim sparse-mode
```

To enable PIM-SM on ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip pim sparse-mode
```

To enable PIM-SM on ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip pim sparse-mode
```

# ip pim sparse-mode join-prune-batching

**Overview** Use this command to enable batching of Join and Prune messages in PIM-SM. This functionality reduces the number of PIM packets that must be sent to maintain a large number of groups

Use the **no** variant of this command to disable batching of Join and Prune messages in PIM-SM.

**Syntax** `ip pim sparse-mode join-prune-batching`  
`no ip pim sparse-mode join-prune-batching`

**Default** Disabled.

**Mode** Global Configuration

**Examples** To enable Join/Prune batching for PIM-SM, use the commands:

```
awplus# configure terminal
awplus(config)# ip pim sparse-mode join-prune-batching
```

To disable Join/Prune batching for PIM-SM, use the commands:

```
awplus# configure terminal
awplus(config)# no ip pim sparse-mode join-prune-batching
```

**Related commands** [ip pim sparse-mode wrong-vif-suppression](#)

**Command changes** Version 5.4.8-2.3: command added.

# ip pim sparse-mode passive

**Overview** Use this command to enable and disable passive mode operation for local members on an interface.

Use the **no** variant of this command to disable passive mode operation for local members on an interface.

**Syntax** ip pim sparse-mode passive  
no ip pim sparse-mode passive

**Mode** Interface Configuration for a Eth or a PPP interface.

**Usage** Passive mode essentially stops PIM transactions on the interface, allowing only IGMP mechanism to be active. To turn off passive mode, use the **no ip pim sparse-mode passive** or the **ip pim sparse-mode** command. To turn off PIM activities on an interface, use the **no ip pim sparse-mode** command.

**Examples** To enable passive mode on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip pim sparse-mode passive
```

To disable passive mode on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ip pim sparse-mode passive
```

To enable passive mode on ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip pim sparse-mode passive
```

To disable passive mode on ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip pim sparse-mode passive
```



# ip pim sparse-mode wrong-vif-suppression

**Overview** Use this command to permit or block multicast packets that arrive on the wrong interface.

Use the **no** variant of this command to disable wrong VIF suppression.

**Syntax** `ip pim sparse-mode wrong-vif-suppression`  
`no ip pim sparse-mode wrong-vif-suppression`

**Default** Disabled.

**Mode** Global Configuration

**Usage notes** This command enables wrong VIF suppression for PIM sparse-mode. Wrong VIF suppression prevents multicast packets received on the wrong upstream interface from being copied to the CPU.

**Examples** To enable wrong VIF suppression, use the commands:

```
awplus# configure terminal
awplus(config)# ip pim sparse-mode wrong-vif-suppression
```

To disable wrong VIF suppression, use the commands:

```
awplus# configure terminal
awplus(config)# no ip pim sparse-mode wrong-vif-suppression
```

**Related commands** [ip pim sparse-mode join-prune-batching](#)

**Command changes** Version 5.4.8-2.3: command added.

# ip pim spt-threshold

**Overview** This command turns on the ability for the last-hop PIM router to switch to SPT (shortest-path tree).  
The **no** variant of this command turns off the ability for the last-hop PIM router to switch to SPT.

**NOTE:** *The switching to SPT happens either at the receiving of the first data packet, or not at all; it is not rate-based.*

**Syntax** ip pim spt-threshold  
no ip pim spt-threshold

**Mode** Global Configuration

**Examples** To enable the last-hop PIM-SM router to switch to SPT, use the following commands:

```
awplus# configure terminal
awplus(config)# ip pim spt-threshold
```

To stop the last-hop PIM-SM router from being able to switch to SPT, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip pim spt-threshold
```

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# ip pim ssm

**Overview** Use this command to define the Source Specific Multicast (SSM) range of IP multicast addresses. The default keyword defines the SSM range as 232/8.

Use the **no** variant of this command to disable the SSM range.

**Syntax** `ip pim ssm default`  
`no ip pim ssm`

| Parameter | Description                     |
|-----------|---------------------------------|
| default   | Use 232/8 as the range for SSM. |

**Default** By default, the command is disabled.

**Mode** Global Configuration

**Usage** When an SSM range of IP multicast addresses is defined by this command, the no (\*,G) or (S,G,rpt) state will be initiated for groups in the SSM range.

The messages corresponding to these states will not be accepted or originated in the SSM range.

**Examples** To use the default address range for PIM-SSM, use the commands:

```
awplus# configure terminal
awplus(config)# ip pim ssm default
```

To disable PIM-SSM, use the commands:

```
awplus# configure terminal
awplus(config)# no ip pim ssm
```

**Command changes** Version 5.5.3-1.1: VRF-lite support added.

# service pim

**Overview** Use this command to enable PIM sparse mode services.  
Use the **no** version of the command to disable unused PIM sparse mode services.

**Syntax** `service pim`  
`no service pim`

**Default** Enabled

**Mode** Global Configuration

**Usage notes** Sometimes it may be desirable to disable unused services, in order to reduce memory use.  
Disabling the PIM services will only take effect after you save the configuration and restart the device.

**Example** To disable the PIM sparse mode service, use the commands:

```
awplus# configure terminal
awplus(config)# no service pim
```

**Output** Figure 31-3: Example output from **no service pim**

```
awplus(config)#no service pim
% Save the config and restart the device for this change to take
effect
```

**Command changes** Version 5.5.0-0.1: command added

# show debugging pim sparse-mode

**Overview** This command displays the status of the debugging of the system.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show debugging pim sparse-mode

**Mode** User Exec and Privileged Exec

**Example** To display PIM-SM debugging settings, use the command:

```
awplus# show debugging pim sparse-mode
```

Figure 31-4: Output from **show debugging pim sparse-mode**

```
Debugging status:
PIM event debugging is on
PIM Hello THT timer debugging is on
PIM event debugging is on
PIM MFC debugging is on
PIM state debugging is on
PIM packet debugging is on
PIM incoming packet debugging is on
PIM outgoing packet debugging is on
```

**Related commands** [debug pim sparse-mode](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# show ip pim sparse-mode bsr-router

**Overview** Use this command to show the Bootstrap Router (BSR) (v2) address.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip pim sparse-mode bsr-router`

**Mode** User Exec and Privileged Exec

**Output** Figure 31-5: Output from the **show ip pim sparse-mode bsr-router** command

```
PIMv2 Bootstrap information
BSR address: 10.10.11.35 (?)
Uptime: 00:00:38, BSR Priority: 0, Hash mask length: 10
Expires: 00:01:32
Role: Non-candidate BSR
State: Accept Preferred
```

**Related commands** [show ip pim sparse-mode rp mapping](#)  
[show ip pim sparse-mode neighbor](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# show ip pim sparse-mode interface

**Overview** Use this command to show PIM-SM interface information.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#)

**Syntax** `show ip pim sparse-mode interface`

**Mode** User Exec and Privileged Exec

**Example** To display information about PIM-SM interfaces, use the command:

```
awplus# show ip pim sparse-mode interface
```

**Output** Figure 31-6: Example output from **show ip pim sparse-mode interface**

| Total configured interfaces: 16    Maximum allowed: 31 |           |          |              |              |             |               |
|--------------------------------------------------------|-----------|----------|--------------|--------------|-------------|---------------|
| Total active interfaces:        12                     |           |          |              |              |             |               |
| Address                                                | Interface | VIFindex | Ver/<br>Mode | Nbr<br>Count | DR<br>Prior | DR            |
| 192.168.1.53                                           | eth0      | 0        | v2/S         | 2            | 2           | 192.168.1.53  |
| 192.168.10.53                                          | eth1      | 2        | v2/S         | 0            | 2           | 192.168.10.53 |
| ...                                                    |           |          |              |              |             |               |

**Table 1:** Parameters in the output from the **show ip pim sparse-mode interface** command

| Parameters                  | Description                                                              |
|-----------------------------|--------------------------------------------------------------------------|
| Total configured interfaces | The number of configured PIM Sparse Mode interfaces.                     |
| Maximum allowed             | The maximum number of PIM Sparse Mode interfaces that can be configured. |
| Total active interfaces     | The number of active PIM Sparse Mode interfaces.                         |
| Address                     | Primary PIM-SM address.                                                  |
| Interface                   | Name of the PIM-SM interface.                                            |
| VIF Index                   | The Virtual Interface index of the interface.                            |
| Ver/Mode                    | PIM version/Sparse mode.                                                 |
| Nbr Count                   | Neighbor count of the PIM-SM interface.                                  |

**Table 1:** Parameters in the output from the **show ip pim sparse-mode interface** command (cont.)

| Parameters  | Description                              |
|-------------|------------------------------------------|
| DR Priority | Designated Router priority.              |
| DR          | The IP address of the Designated Router. |

**Related  
commands**

[ip pim sparse-mode](#)  
[show ip pim sparse-mode rp mapping](#)  
[show ip pim sparse-mode neighbor](#)

**Command  
changes**

Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.



# show ip pim sparse-mode interface detail

**Overview** Use this command to show detailed information on a PIM-SM interface.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip pim sparse-mode interface detail`

**Mode** User Exec and Privileged Exec

**Output** Figure 31-7: Example output from the **show ip pim sparse-mode interface detail** command

```
eth1 (vif 3):
 Address 192.168.1.149, DR 192.168.1.149
 Hello period 30 seconds, Next Hello in 15 seconds
 Triggered Hello period 5 seconds
 Neighbors:
 192.168.1.22

eth0 (vif 0):
 Address 10.10.11.149, DR 10.10.11.149
 Hello period 30 seconds, Next Hello in 18 seconds
 Triggered Hello period 5 seconds
 Neighbors:
 10.10.11.4
```

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# show ip pim sparse-mode local-members

**Overview** Use this command to show detailed local member information on an interface configured for PIM-SM. If you do not specify an interface then detailed local member information is shown for all interfaces configured for PIM-SM.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip pim sparse-mode local-members [<interface>]`

| Parameter   | Description                      |
|-------------|----------------------------------|
| <interface> | Optional. Specify the interface. |

**Mode** User Exec and Privileged Exec

**Example** To show detailed PIM-SM information for all PIM-SM configured interfaces, use the command:

```
awplus# show ip pim sparse-mode local-members
```

To show detailed PIM-SM information for the PIM-SM configured interface eth1, use the command:

```
awplus# show ip pim sparse-mode local-members eth1
```

**Output** Figure 31-8: Example output from the **show ip pim sparse-mode local-members** command

```
awplus#show ip pim sparse-mode local-members
PIM Local membership information

eth0:
 (*, 224.0.0.4) : Include

eth1:
 (*, 223.0.0.3) : Include
```

**Output** Figure 31-9: Example output from the **show ip pim sparse-mode local-members** command on a specific interface.

```
awplus#show ip pim sparse-mode local-members eth11
PIM Local membership information

eth11:
 (*, 224.0.0.4) : Include
```

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# show ip pim sparse-mode mroute

**Overview** Use this command to display the IP multicast routing table or the IP multicast routing table based on a specific address or addresses.

**Syntax**

```
show ip pim sparse-mode mroute brief
show ip pim sparse-mode mroute
show ip pim sparse-mode mroute <group-address>
show ip pim sparse-mode mroute <source-address>
show ip pim sparse-mode mroute <source-address> <group-address>
```

| Parameter        | Description                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------|
| brief            | Shows only a summary of the number of each type of multicast entry and the cache.                         |
| <group-address>  | Group IP address, entered in the form A.B.C.D. Output is all multicast entries belonging to that group.   |
| <source-address> | Source IP address, entered in the form A.B.C.D. Output is all multicast entries belonging to that source. |

**Mode** Privileged Exec

**Usage notes** Note that when a feature license is enabled, the output for the **show ip pim sparse-mode mroute** command will only show 32 interfaces because of the terminal display width limit. Use the **show ip pim sparse-mode mroute detail** command to display detailed entries of the IP multicast routing table.

**Example** To display the IP multicast routing table for the address 40.40.40.11, enter the command:

```
awplus# show ip pim sparse-mode mroute 40.40.40.11
```

**Output** Figure 31-10: Example output from **show ip pim sparse-mode mroute brief**

```
awplus#show ip pim sparse-mode mroute brief
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 99
(S,G,rpt) Entries: 99
FCR Entries: 0
MRIB Msg Cache Hit: 0
```

**Output** Figure 31-11: Example output from **show ip pim sparse-mode mroute**

```
awplus#show ip pim sparse-mode mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 99
(S,G,rpt) Entries: 99
FCR Entries: 0
MRIB Msg Cache Hit: 0

(10.200.0.2, 224.1.1.1)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
 Local 1
 Joined 0
 Asserted Winner 0
 Asserted Loser 0
 Outgoing 1
 Interop listener rx-data flags (ES,EDW,RXD,DAJ,EOE)
 0x00000000 0x00000000 0x00000001
(10.200.0.2, 224.1.1.1, rpt)
RP: 0.0.0.0
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: RPT NOT JOINED
 Local 0
 Pruned 0
 Outgoing 0
 Interop listener rx-data flags (ES,EDW,RXD,DAJ,EOE)
 0x00000000 0x00000000 0x00000001
...
```

**Related commands** [show ip pim sparse-mode mroute detail](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added to SBx8100.  
Version 5.4.8-1.1: VRF-lite support added to x930, SBx908 GEN2.  
Version 5.4.8-2.1: **brief** parameter added.

# show ip pim sparse-mode mroute detail

**Overview** Use this command to display detailed entries of the IP multicast routing table, or detailed entries of the IP multicast routing table based on the specified address or addresses.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax**

```
show ip pim sparse-mode mroute [<group-address>] detail
show ip pim sparse-mode mroute [<source-address>] detail
show ip pim sparse-mode mroute [<group-address>
<source-address>] detail
show ip pim sparse-mode mroute [<source-address>
<group-address>] detail
```

| Parameter        | Description                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------|
| <group-address>  | Group IP address, entered in the form A.B.C.D. Output is all multicast entries belonging to that group.   |
| <source-address> | Source IP address, entered in the form A.B.C.D. Output is all multicast entries belonging to that source. |
| detail           | Show detailed information.                                                                                |

**Usage notes** Based on the group and source address, the output is the selected route if present in the multicast route tree.

**Mode** User Exec and Privileged Exec

**Examples** The following example commands show detailed entries for IP multicast routing tables:

```
awplus# show ip pim sparse-mode mroute detail
awplus# show ip pim sparse-mode mroute 40.40.40.11 detail
awplus# show ip pim sparse-mode mroute 224.1.1.1 detail
awplus# show ip pim sparse-mode mroute 224.1.1.1 40.40.40.11
detail
```

**Output** Figure 31-12: Example output from **show ip pim sparse-mode mroute detail**

```
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 4
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.0.1.24) Uptime: 00:06:42
RP: 0.0.0.0, RPF nbr: None, RPF idx: None
Upstream:
 State: JOINED, SPT Switch: Disabled, JT: off
 Macro state: Join Desired,
Downstream:
 eth1:
 State: NO INFO, ET: off, PPT: off
 Assert State: NO INFO, AT: off
 Winner: 0.0.0.0, Metric: 42949672951, Pref: 42949672951,
RPT bit: on
 Macro state: Could Assert, Assert Track
Local Olist:
 eth1
```

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# show ip pim sparse-mode neighbor

**Overview** Use this command to show the PIM-SM neighbor information.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip pim sparse-mode neighbor [<interface>] [<ip-address>]  
[detail]`

| Parameter    | Description                                                                                           |
|--------------|-------------------------------------------------------------------------------------------------------|
| <interface>  | Interface name. Show neighbors on an interface.                                                       |
| <ip-address> | Show neighbors with a particular address on an interface. The IP address entered in the form A.B.C.D. |
| detail       | Show detailed information.                                                                            |

**Mode** Privileged Exec

**Examples** To show the neighbor information for all interfaces, use the command:

```
awplus# show ip pim sparse-mode neighbor
```

To show the neighbor information for eth1, use the command:

```
awplus# show ip pim sparse-mode neighbor eth1 detail
```

**Output** Figure 31-13: Example output from the **show ip pim sparse-mode neighbor** command

| Neighbor Address Mode | Interface | Uptime/Expires    | Ver | DR Priority/ |
|-----------------------|-----------|-------------------|-----|--------------|
| 10.10.0.9             | eth1      | 00:55:33/00:01:44 | v2  | 1 /          |
| 10.10.0.136           | eth1      | 00:55:20/00:01:25 | v2  | 1 /          |
| 10.10.0.172           | eth1      | 00:55:33/00:01:32 | v2  | 1 / DR       |

Figure 31-14: Example output from the **show ip pim sparse-mode neighbor interface detail** command

|                                                                   |
|-------------------------------------------------------------------|
| Nbr 10.10.3.180 (eth1), DR                                        |
| Expires in 55 seconds, uptime 00:00:15                            |
| Holdtime: 70 secs, T-bit: off, lan delay: 1, Override interval: 3 |
| DR priority: 100, Gen ID: 625159467,                              |
| Secondary addresses:                                              |
| 192.168.30.1                                                      |

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.



# show ip pim sparse-mode nexthop

**Overview** Use this command to see the next hop information as used by PIM-SM.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#)

**Syntax** `show ip pim sparse-mode nexthop`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip pim sparse-mode nexthop`

Figure 31-15: Example output from the **show ip pim sparse-mode nexthop** command

| Flags: N = New, R = RP, S = Source, U = Unreachable |      |             |              |         |                 |        |      |        |
|-----------------------------------------------------|------|-------------|--------------|---------|-----------------|--------|------|--------|
| Destination                                         | Type | Nexthop Num | Nexthop Addr | Nexthop | Nexthop Ifindex | Metric | Pref | Refcnt |
| 10.10.0.9                                           | .RS. | 1           | 0.0.0.0      | 4       | 0               | 0      | 1    |        |

**Table 2:** Parameters in output of the **show ip pim sparse-mode nexthop** command

| Parameter       | Description                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------|
| Destination     | The destination address for which PIM-SM requires next hop information.                                      |
| Type            | The type of destination, as indicated by the Flags description. N = New, R= RP, S = Source, U = Unreachable. |
| Nexthop Num     | The number of next hops to the destination. PIM-SM always uses only 1 next hop.                              |
| Nexthop Addr    | The address of the primary next hop gateway.                                                                 |
| Nexthop IfIndex | The interface on which the next hop gateway can be reached.                                                  |
| Nexthop Name    | The name of next hop interface.                                                                              |
| Metric          | The metric of the route towards the destination.                                                             |
| Preference      | The preference of the route towards destination.                                                             |
| Refcnt          | Only used for debugging.                                                                                     |

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.

Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# show ip pim sparse-mode packet statistics

**Overview** Use this command to display the current packet receive counts for PIM sparse-mode.

**Syntax** `show ip pim sparse-mode packet statistics`

**Mode** Privileged Exec

**Example** The following command displays the current packet receive counts for PIM sparse-mode:

```
awplus# configure terminal
awplus(config)# show ip pim sparse-mode statistics
```

**Output** Figure 31-16: Example output from **show ip pim sparse-mode statistics**

```
awplus(config)#show ip pim sparse-mode statistics
PIM-SM Receive Packet Statistics :
All PIM-SM : Total : 25 Valid : 25
Hello : Total : 14 Valid : 14
Register : Total : 5 Valid : 5
Register Stop : Total : 0 Valid : 0
Join/Prune : Total : 0 Valid : 0
Bootstrap : Total : 6 Valid : 6
Assert : Total : 0 Valid : 0
Candidate-RP : Total : 0 Valid : 0
```

**Related commands** [clear ip pim sparse-mode packet statistics](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# show ip pim sparse-mode rp-hash

**Overview** Use this command to display the Rendezvous Point (RP) to be chosen based on the group selected.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip pim sparse-mode rp-hash <group-addr>`

| Parameter                       | Description                                                              |
|---------------------------------|--------------------------------------------------------------------------|
| <code>&lt;group-addr&gt;</code> | The group address for which to find the RP, entered in the form A.B.C.D. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip pim sparse-mode rp-hash 224.0.1.3`

Figure 31-17: Output from the **show ip pim sparse-mode rp-hash** command

```
RP: 10.10.11.35
Info source: 10.10.11.35, via bootstrap
```

**Related commands** [show ip pim sparse-mode rp mapping](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# show ip pim sparse-mode rp mapping

**Overview** Use this command to show group-to-RP (Rendezvous Point) mappings, and the RP set.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip pim sparse-mode rp mapping`

**Mode** Privileged Exec

**Example** `awplus# show ip pim sparse-mode rp mapping`

**Output** Figure 31-18: Example output from **show ip pim sparse-mode rp mapping**

```
PIM Group-to-RP Mappings
Group(s) : 224.0.0.0/4
RP: 10.10.0.9
 Info source: 10.10.0.9, via bootstrap, priority 192
 Uptime: 16:52:39, expires: 00:02:50
```

**Related commands** [show ip pim sparse-mode rp-hash](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

# undebug all pim sparse-mode

**Overview** Use this command to disable all PIM-SM debugging.

**Syntax** `undebug all pim sparse-mode`

**Mode** Privileged Exec

**Example** `awplus# undebug all pim sparse-mode`

**Related commands** [debug pim sparse-mode](#)

**Command changes** Version 5.4.7-1.1: VRF-lite support added SBx8100.  
Version 5.4.8-1.1: VRF-lite support added x930, SBx908 GEN2.

## Introduction

**Overview** This chapter provides an alphabetical reference of PIM-SMv6 commands. For IPv6 Multicast commands, see [Multicast Commands](#). For an overview of PIM-SMv6, see the [PIM-SMv6 Feature Overview and Configuration Guide](#).

IPv6 must be enabled on an interface with the [ipv6 enable](#) command, IPv6 forwarding must be enabled globally for routing IPv6 with the [ipv6 forwarding](#) command, and IPv6 multicasting must be enabled globally with the [ipv6 multicast-routing](#) command before using PIM-SMv6 commands.

Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the [clear ipv6 mroute](#) command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous IPv6 static multicast routes.

**NOTE:** The IPv6 Multicast addresses shown can be derived from IPv6 unicast prefixes as per RFC 3306. The IPv6 unicast prefix reserved for documentation is 2001:0db8::/32 as per RFC 3849. Using the base /32 prefix the IPv6 multicast prefix for 2001:0db8::/32 is ff3x:20:2001:0db8::/64. Where an RP address is 2001:0db8::1 the embedded RP multicast prefix is ff7x:120:2001:0db8::/96. For ASM (Any-Source Multicast) the IPv6 multicast addresses allocated for documentation purposes are ff0x::0db8:0:0/96 as per RFC 6676. This is a /96 prefix so that it can be used with group IDs as per RFC 3307. These addresses should not be used for practical networks (other than for testing purposes), nor should they appear in any public network.

The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.

- Command List**
- [“clear ipv6 mroute pim”](#) on page 1469
  - [“clear ipv6 mroute pim sparse-mode”](#) on page 1470
  - [“clear ipv6 pim sparse-mode bsr rp-set \\*”](#) on page 1471
  - [“debug ipv6 pim sparse-mode”](#) on page 1472

- [“debug ipv6 pim sparse-mode packet”](#) on page 1474
- [“debug ipv6 pim sparse-mode timer”](#) on page 1475
- [“ipv6 pim anycast-rp”](#) on page 1477
- [“ipv6 pim bsr-border”](#) on page 1479
- [“ipv6 pim bsr-candidate”](#) on page 1481
- [“ipv6 pim cisco-register-checksum”](#) on page 1483
- [“ipv6 pim crp-cisco-prefix”](#) on page 1484
- [“ipv6 pim dr-priority”](#) on page 1485
- [“ipv6 pim exclude-genid”](#) on page 1487
- [“ipv6 pim ext-srcs-directly-connected”](#) on page 1488
- [“ipv6 pim hello-holdtime”](#) on page 1489
- [“ipv6 pim hello-interval”](#) on page 1491
- [“ipv6 pim ignore-rp-set-priority”](#) on page 1492
- [“ipv6 pim jp-timer”](#) on page 1493
- [“ipv6 pim register-rate-limit”](#) on page 1494
- [“ipv6 pim register-rp-reachability”](#) on page 1495
- [“ipv6 pim register-source”](#) on page 1496
- [“ipv6 pim register-suppression”](#) on page 1498
- [“ipv6 pim rp-address”](#) on page 1499
- [“ipv6 pim rp-candidate”](#) on page 1500
- [“ipv6 pim rp embedded”](#) on page 1501
- [“ipv6 pim rp-register-kat”](#) on page 1502
- [“ipv6 pim sparse-mode”](#) on page 1503
- [“ipv6 pim sparse-mode passive”](#) on page 1504
- [“ipv6 pim spt-threshold”](#) on page 1505
- [“ipv6 pim ssm”](#) on page 1506
- [“ipv6 pim unicast-bsm”](#) on page 1507
- [“service pim6”](#) on page 1508
- [“show debugging ipv6 pim sparse-mode”](#) on page 1509
- [“show ipv6 pim sparse-mode bsr-router”](#) on page 1510
- [“show ipv6 pim sparse-mode interface”](#) on page 1511
- [“show ipv6 pim sparse-mode interface detail”](#) on page 1513
- [“show ipv6 pim sparse-mode local-members”](#) on page 1514
- [“show ipv6 pim sparse-mode mroute”](#) on page 1515
- [“show ipv6 pim sparse-mode mroute detail”](#) on page 1517

- [“show ipv6 pim sparse-mode neighbor”](#) on page 1519
- [“show ipv6 pim sparse-mode nexthop”](#) on page 1520
- [“show ipv6 pim sparse-mode rp-hash”](#) on page 1522
- [“show ipv6 pim sparse-mode rp mapping”](#) on page 1523
- [“show ipv6 pim sparse-mode rp nexthop”](#) on page 1524
- [“undebug all ipv6 pim sparse-mode”](#) on page 1526
- [“undebug ipv6 pim sparse-mode”](#) on page 1527



# clear ipv6 mroute pim

**Overview** Use this command to clear all Multicast Forwarding Cache (MFC) entries in PIM-SMv6.

**NOTE:** Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the *clear ipv6 mroute* command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.

**Syntax** `clear ipv6 mroute [*] pim sparse-mode`

| Parameter | Description                                                                                                                              |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------|
| *         | Clears all PIM-SMv6 multicast routes. Using this command without this optional operator only deletes the multicast router table entries. |

**Mode** Privileged Exec

**Example** `awplus# clear ipv6 mroute pim sparse-mode`  
`awplus# clear ipv6 mroute * pim sparse-mode`

# clear ipv6 mroute pim sparse-mode

**Overview** Use this command to clear all multicast route table entries learned through PIM-SMv6 for a specified multicast group address, and optionally a specified multicast source address.

**NOTE:** Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the *clear ipv6 mroute* command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.

**Syntax** `clear ipv6 mroute <Group-IPv6-add> pim sparse-mode`  
`clear ipv6 mroute <Group-IPv6-add> <Source-IPv6-add> pim sparse-mode`

| Parameter         | Description                                                           |
|-------------------|-----------------------------------------------------------------------|
| <Group-IPv6-add>  | Specify a multicast group IPv6 address, entered in the form X:X::X:X. |
| <Source-IPv6-add> | Specify a source group IPv6 address, entered in the form X:X::X:X.    |

**Mode** Privileged Exec

**Example** `awplus# clear ipv6 mroute 2001:db8:: pim sparse-mode`  
`awplus# clear ipv6 mroute 2001:db8:: 2002:db8:: pim sparse-mode`

# clear ipv6 pim sparse-mode bsr rp-set \*

**Overview** Use this command to clear all Rendezvous Point (RP) sets learned through the PIM-SMv6 Bootstrap Router (BSR).

**NOTE:** Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the [clear ipv6 mroute](#) command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.

**Syntax** `clear ipv6 pim sparse-mode bsr rp-set *`

| Parameter | Description         |
|-----------|---------------------|
| *         | Clears all RP sets. |

**Mode** Privileged Exec

**Usage** For multicast clients, note that one router will be automatically or statically designated as the RP, and all routers must explicitly join through the RP. A Designated Router (DR) sends periodic Join/Prune messages toward a group-specific RP for each group that it has active members.

For multicast sources, note that the Designated Router (DR) unicasts Register messages to the RP encapsulating the data packets from the multicast source. The RP forwards decapsulated data packets toward group members.

**Example** `awplus# clear ipv6 pim sparse-mode bsr rp-set *`

# debug ipv6 pim sparse-mode

**Overview** Use this command to activate PIM-SMv6 debugging.

Use the **no** variant of this command to deactivate PIMv6 debugging.

Note that the **undebg ipv6 pim sparse-mode** command is an alias of the **no** variant of this command.

**Syntax** `debug ipv6 pim sparse-mode [all] [events] [mfc] [mib] [nexthop]  
[nsm] [state] [timer]`  
`no debug ipv6 pim sparse-mode [all] [events] [mfc] [mib]  
[nexthop] [nsm] [state] [timer]`

| Parameter | Description                                                                   |
|-----------|-------------------------------------------------------------------------------|
| all       | Activates/deactivates all PIM-SMv6 debugging.                                 |
| events    | Activates debug printing of PIM-SMv6 events.                                  |
| mfc       | Activates debug printing of MFC (Multicast Forwarding Cache).                 |
| mib       | Activates debug printing of PIM-SMv6 MIBs.                                    |
| nexthop   | Activates debug printing of PIM-SMv6 next hop communications.                 |
| nsm       | Activates debugging of PIM-SMv6 NSM (Network Services Module) communications. |
| state     | Activates debug printing of state transition on all PIM-SMv6 FSMs.            |
| timer     | Activates debug printing of PIM-SMv6 timers.                                  |

**Mode** Privileged Exec and Global Configuration

**Example** `awplus# configure terminal  
awplus(config)# terminal monitor  
awplus(config)# debug ipv6 pim sparse-mode all  
awplus# configure terminal  
awplus(config)# terminal monitor  
awplus(config)# debug ipv6 pim sparse-mode events  
awplus# configure terminal  
awplus(config)# terminal monitor  
awplus(config)# debug ipv6 pim sparse-mode nexthop`

**Validation  
output**

Figure 32-1: Example output from the **show debugging ipv6 pim sparse-mode** command after issuing **multiple debug ipv6 pim sparse-mode** commands

```
awplus#debug ipv6 pim sparse-mode state
awplus#debug ipv6 pim sparse-mode events
awplus#debug ipv6 pim sparse-mode packet
awplus#show debugging ipv6 pim sparse-mode
PIM-SMv6 debugging status:
 PIM event debugging is on
 PIM MFC debugging is off
 PIM state debugging is on
 PIM packet debugging is on
 PIM Hello HT timer debugging is off
 PIM Hello NLT timer debugging is off
 PIM Hello THT timer debugging is off
 PIM Join/Prune JT timer debugging is off
 PIM Join/Prune ET timer debugging is off
 PIM Join/Prune PPT timer debugging is off
 PIM Join/Prune KAT timer debugging is off
 PIM Join/Prune OT timer debugging is off
 PIM Assert AT timer debugging is off
 PIM Register RST timer debugging is off
 PIM Bootstrap BST timer debugging is off
 PIM Bootstrap CRP timer debugging is off
 PIM mib debugging is off
 PIM nsm debugging is off
 PIM nexthop debugging is off
```

**Related  
commands**

[show debugging ipv6 pim sparse-mode](#)  
[undebug all ipv6 pim sparse-mode](#)  
[undebug ipv6 pim sparse-mode](#)

# debug ipv6 pim sparse-mode packet

**Overview** Use this command to activate PIM-SMv6 packet debugging.  
Use the no variant of this command to deactivate PIMv6 packet debugging.

**Syntax** debug ipv6 pim sparse-mode packet {in|out}  
no debug ipv6 pim sparse-mode packet {in|out}

| Parameter | Description                                                        |
|-----------|--------------------------------------------------------------------|
| packet    | Activates debug printing of incoming and/or outgoing IPv6 packets. |
| in        | Specify incoming packet debugging.                                 |
| out       | Specify outgoing packet debugging.                                 |

**Mode** Privileged Exec and Global Configuration

**Example**

```
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# debug ipv6 pim sparse-mode packet in
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# debug ipv6 pim sparse-mode packet out
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# no debug ipv6 pim sparse-mode packet in
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# no debug ipv6 pim sparse-mode packet out
```

**Related commands** [show debugging ipv6 pim sparse-mode](#)  
[undebug all ipv6 pim sparse-mode](#)

# debug ipv6 pim sparse-mode timer

**Overview** Use this command to enable debugging for the specified PIM-SMv6 timers.

Use the **no** variants of this command to disable debugging for the specified PIM-SMv6 timers.

**Syntax**

```
debug ipv6 pim sparse-mode timer assert [at]
no debug ipv6 pim sparse-mode timer assert [at]
debug pim ipv6 sparse-mode timer bsr [bst|crp]
no debug pim ipv6 sparse-mode timer bsr [bst|crp]
debug pim ipv6 sparse-mode timer hello [ht|nlt|tht]
no debug pim ipv6 sparse-mode timer hello [ht|nlt|tht]
debug pim ipv6 sparse-mode timer joinprune [jt|et|ppt|kat|ot]
no debug pim ipv6 sparse-mode timer joinprune
[jt|et|ppt|kat|ot]
debug pim ipv6 sparse-mode timer register [rst]
no debug pim ipv6 sparse-mode timer register [rst]
```

| Parameter | Description                                                                                           |
|-----------|-------------------------------------------------------------------------------------------------------|
| assert    | Enable or disable debugging for the Assert timers.                                                    |
| at        | Enable or disable debugging for the Assert Timer.                                                     |
| bsr       | Enable or disable debugging for the specified Bootstrap Router timer, or all Bootstrap Router timers. |
| bst       | Enable or disable debugging for the Bootstrap Router: Bootstrap Timer.                                |
| crp       | Enable or disable debugging for the Bootstrap Router: Candidate-RP Timer.                             |
| hello     | Enable or disable debugging for the specified Hello timer, or all Hello timers.                       |
| ht        | Enable or disable debugging for the Hello timer: Hello Timer.                                         |
| nlt       | Enable or disable debugging for the Hello timer: Neighbor Liveness Timer.                             |
| tht       | Enable or disable debugging for the Hello timer: Triggered Hello Timer.                               |
| joinprune | Enable or disable debugging for the specified JoinPrune timer, or all JoinPrune timers.               |
| jt        | Enable or disable debugging for the JoinPrune timer: upstream Join Timer.                             |
| et        | Enable or disable debugging for the JoinPrune timer: Expiry Timer.                                    |
| ppt       | Enable or disable debugging for the JoinPrune timer: PrunePending Timer.                              |

| Parameter | Description                                                                   |
|-----------|-------------------------------------------------------------------------------|
| kat       | Enable or disable debugging for the JoinPrune timer: KeepAlive Timer.         |
| ot        | Enable or disable debugging for the JoinPrune timer: Upstream Override Timer. |
| register  | Enable or disable debugging for the Register timers.                          |
| rst       | Enable or disable debugging for the Register timer: Register Stop Timer.      |

**Default** By default, all debugging is disabled.

**Mode** Privileged Exec and Global Configuration

**Examples** To enable debugging for the PIM-SMv6 Bootstrap Router bootstrap timer, use the commands:

```
awplus(config)# debug ipv6 pim sparse-mode timer bsr bst
```

To enable debugging for the PIM-SMv6 Hello: neighbor liveness timer, use the command:

```
awplus(config)# debug ipv6 pim sparse-mode timer hello ht
```

To enable debugging for the PIM-SMv6 Joinprune expiry timer, use the command:

```
awplus# debug ipv6 pim sparse-mode timer joinprune et
```

To disable debugging for the PIM-SMv6 Register timer, use the command:

```
awplus# no debug ipv6 pim sparse-mode timer register
```

**Related commands** [show debugging ipv6 pim sparse-mode](#)



# ipv6 pim anycast-rp

**Overview** Use this command to configure Anycast RP (Rendezvous Point) in an RP set.  
Use the **no** variant of this command to remove the configuration.

**Syntax** `ipv6 pim anycast-rp <anycast-rp-address> <member-rp-address>`  
`no ipv6 pim anycast-rp <anycast-rp-address>`  
`[<member-rp-address>]`

| Parameter                               | Description                                                                                                                 |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;anycast-rp-address&gt;</code> | <code>&lt;X:X::X:X&gt;</code> Specify an Anycast IPv6 address to configure an Anycast RP (Rendezvous Point) in a RP set.    |
| <code>&lt;member-rp-address&gt;</code>  | <code>&lt;A:B::C:D&gt;</code> Specify an Anycast RP (Rendezvous Point) IPv6 address to configure an Anycast RP in a RP set. |

**Mode** Global Configuration

**Usage notes** Anycast is a network addressing and routing scheme where data is routed to the nearest or best destination as viewed by the routing topology. Compared to unicast with a one-to-one association between network address and network endpoint, and multicast with a one-to-many association between network address and network endpoint; anycast has a one-to-many association between network address and network endpoint. For anycast, each destination address identifies a set of receiver endpoints, from which only one receiver endpoint is chosen.

Anycast is often implemented using BGP to simultaneously advertise the same destination IPv6 address range from many sources, resulting in packets addressed to destination addresses in this range being routed to the nearest source announcing the given destination IPv6 address.

Use this command to specify the Anycast RP configuration in the Anycast RP set. Use the **no** variant of this command to remove the Anycast RP configuration. Note that the member RP address is optional when using the **no** parameter to remove the Anycast RP configuration. Removing the Anycast RP address also removes the member RP address.

**Examples** The following example shows how to configure the Anycast RP address with **ipv6 pim anycast-rp**:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim anycast-rp 2:2::2:2 20:20::20:20
```

The following example shows how to remove the Anycast RP in the RP set specifying only the Anycast RP address with **no ipv6 pim anycast-rp**, but not specifying the member RP address:

```
awplus# configure terminal
awplus(config)# no ipv6 pim anycast-rp 2:2::2:2 20:20::20:20
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim bsr-border

**Overview** Use the **ipv6 pim bsr-border** command to prevent Bootstrap Router (BSR) messages from being sent or received through an interface. The BSR border is the border of the PIM-SMv6 domain.

Use the **no** variant of this command to disable the configuration set with **ipv6 pim bsr-border**.

**Syntax** `ipv6 pim bsr-border`  
`no ipv6 pim bsr-border`

**Mode** Interface Configuration for an Eth or PPP interface.

**Usage** When this command is configured on an interface, no PIM-SMv6 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM-SMv6 domain with this command to avoid BSR messages from being exchanged between the two PIM-SMv6 domains.

BSR messages should not be exchanged between different domains, because devices in one domain may elect Rendezvous Points (RPs) in the other domain, resulting in loss of isolation between the two PIM domains that would stop the PIM-SMv6 protocol from working as intended.

**Examples** The following example configures the interface eth1 to be the PIM-SMv6 domain border:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim bsr-border
```

The following example removes the interface eth1 from the PIM-SMv6 domain border:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 pim bsr-border
```

The following example configures the PPP interface ppp0 to be the PIM -SMv6 domain border:

```
awplus(config)# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface ppp0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim bsr-border
```

The following example removes the PPP interface ppp0 from the PIM-SMv6 domain border:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 pim bsr-border
```

# ipv6 pim bsr-candidate

**Overview** Use this command to give the device the candidate BSR (Bootstrap Router) status using the specified IPv6 address mask of the interface.

Use the **no** variant of this command to withdraw the address of the interface from being offered as a BSR candidate.

**Syntax** `ipv6 pim bsr-candidate <interface> [<hash>] [<priority>]`  
`no ipv6 pim bsr-candidate [<interface>]`

| Parameter   | Description                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface> | Specify the interface.                                                                                                                                                                                      |
| <hash>      | <0-128> configure the hash mask length used for RP selection. The default hash value if you do not configure this parameter is 126.                                                                         |
| <priority>  | <0-255> configure priority for a BSR candidate. Note that you must also specify the <hash> (mask length) when specifying the <priority>. The default priority if you do not configure this parameter is 64. |

**Mode** Global Configuration

**Default** The default hash parameter value is 126 and the default priority parameter value is 64.

**Examples** To set the BSR candidate to the interface eth1, with the optional mask length and BSR priority parameters, enter the commands shown below:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim bsr-candidate eth1 20 30
```

To withdraw the address of eth1 from being offered as a BSR candidate, enter:

```
awplus# configure terminal
awplus(config)# no ipv6 pim bsr-candidate eth1
```

To set the BSR candidate to the PPP interface ppp0, with the optional mask length and BSR priority parameters, enter the commands shown below:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim bsr-candidate ppp0 20 30
```

To withdraw the address of ppp0 from being offered as a BSR candidate, enter:

```
awplus# configure terminal
```

```
awplus(config)# no ipv6 pim bsr-candidate ppp0
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim cisco-register-checksum

**Overview** Use this command to configure the option to calculate the Register Checksum over the whole packet. This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to disable this option.

**Syntax** `ipv6 pim cisco-register-checksum`  
`no ipv6 pim cisco-register-checksum`

**Default** This command is disabled by default. By default, Register Checksum is calculated only over the header.

**Mode** Global Configuration

**Example** To calculate the Register Checksum over the whole packet, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim cisco-register-checksum
```

To return to calculating the Register Checksum over the header, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim cisco-register-checksum
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim crp-cisco-prefix

**Overview** Use this command to interoperate with Cisco devices that conform to an earlier draft standard. Some Cisco devices might not accept candidate RPs with a group prefix number of zero. Note that the latest BSR specification prohibits sending RP advertisements with prefix 0.

Use the **no** variant of this command to revert to the default settings.

**Syntax** `ipv6 pim crp-cisco-prefix`  
`no ipv6 pim crp-cisco-prefix`

**Mode** Global Configuration

**Example** To enable this option, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim crp-cisco-prefix
```

To disable this option again, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim crp-cisco-prefix
```

**Related commands** [ipv6 pim rp-candidate](#)

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2



# ipv6 pim dr-priority

**Overview** Use this command to set the Designated Router priority value.  
Use the **no** variant of this command to disable this function.

**Syntax** `ipv6 pim dr-priority <priority>`  
`no ipv6 pim dr-priority [<priority>]`

| Parameter  | Description                                                                                                                                      |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <priority> | Specify the Designated Router priority value, in the range 0 to 4294967294. Note that a higher value has a higher preference or higher priority. |

**Default** The default value is 1. The negated form of this command restores the value to the default.

**Mode** Interface Configuration for an Eth or PPP interface.

**Examples** To set the Designated Router priority value to 11234 for the interface eth1, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim dr-priority 11234
```

To disable the Designated Router priority value for the interface eth1, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 pim dr-priority
```

To set the Designated Router priority value to 11234 for the PPP interface ppp0, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface ppp0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim dr-priority 11234
```

To disable the Designated Router priority value for the PPP interface ppp0, apply the commands as shown below:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 pim dr-priority
```

**Related commands** [ipv6 pim ignore-rp-set-priority](#)

# ipv6 pim exclude-genid

**Overview** Use this command to exclude the GenID option from Hello packets sent out by the PIM-SMv6 module on a particular interface. This command is used to inter-operate with older Cisco IOS versions.

Use the **no** variant of this command to revert to default settings.

**Syntax** `ipv6 pim exclude-genid`  
`no ipv6 pim exclude-genid`

**Default** By default, this command is disabled; the GenID option is included.

**Mode** Interface Configuration for an Eth or PPP interface.

**Examples** To exclude the GenID option in Hello packets on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim exclude-genid
```

To include the GenID option in Hello packets, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 pim exclude-genid
```

To exclude the GenID option in Hello packets on ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface ppp0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim exclude-genid
```

# ipv6 pim ext-srcs-directly-connected

**Overview** Use this command to configure PIM-SMv6 to treat all source traffic arriving on the interface as though it was sent from a host directly connected to the interface.

Use the **no** variant of this command to configure PIM-SMv6 to treat only directly connected sources as directly connected.

**Syntax** `ipv6 pim ext-srcs-directly-connected`  
`no ipv6 pim ext-srcs-directly-connected`

**Default** The **no** variant of this command is the default behavior.

**Mode** Interface Configuration for an Eth or PPP interface.

**Example** To configure PIM-SMv6 to treat all sources as directly connected for interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim ext-srcs-directly-connected
```

To configure PIM-SMv6 to treat only directly connected sources as directly connected for interface eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 pim ext-srcs-directly-connected
```

To configure PIM to treat all sources as directly connected for PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface ppp0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim ext-srcs-directly-connected
```

To configure PIM to treat only directly connected sources as directly connected for PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 pim ext-srcs-directly-connected
```

# ipv6 pim hello-holdtime

**Overview** This command configures a hello-holdtime value. You cannot configure a hello-holdtime value that is less than the current hello-interval.

Use the **no** variant of this command to return it to its default of 3.5 \* the current hello-interval.

**Syntax** `ipv6 pim hello-holdtime <holdtime>`  
`no ipv6 pim hello-holdtime`

| Parameter  | Description                                                                      |
|------------|----------------------------------------------------------------------------------|
| <holdtime> | <1-65535><br>The holdtime value in seconds (no fractional seconds are accepted). |

**Default** The default hello-holdtime value is 3.5 \* the current hello-interval. The default hello-holdtime is restored using the negated form of this command.

**Mode** Interface Configuration for an Eth or PPP interface.

**Usage** Each time the hello-interval is updated, the hello-holdtime is also updated, according to the following rules:

If the hello-holdtime is not configured; or if the hello-holdtime is configured and less than the current hello-interval value, it is modified to the (3.5 \* hello-interval). Otherwise, it retains the configured value.

**Examples** To configure a hello-holdtime of 123 seconds on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim hello-holdtime 123
```

To reset the hello-holdtime to default, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 pim hello-holdtime
```

To configure a hello-holdtime of 123 seconds on ppp0, use the commands

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface ppp0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim hello-holdtime 123
```

# ipv6 pim hello-interval

**Overview** This command configures a hello-interval value for PIM-SMv6.

Use the **no** variant of this command to reset the hello-interval for PIM-SMv6 to the default.

**Syntax** `ipv6 pim hello-interval <interval>`  
`no ipv6 pim hello-interval`

| Parameter  | Description                                                      |
|------------|------------------------------------------------------------------|
| <interval> | <1-65535> The value in seconds (no fractional seconds accepted). |

**Default** The default hello-interval value is 30 seconds. The default is restored using the negated form of this command.

**Mode** Interface Configuration for an Eth or PPP interface.

**Usage** When the hello-interval is configured, and the hello-holdtime is not configured, or when the configured hello-holdtime value is less than the new hello-interval value; the holdtime value is modified to the (3.5 \* hello-interval). Otherwise, the hello-holdtime value is the configured value.

**Example** To set the hello-interval to 123 seconds on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim hello-interval 123
```

To set the hello-interval to the default on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 pim hello-interval
```

To set the hello-interval to 123 seconds on ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface ppp0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim hello-interval 123
```

# ipv6 pim ignore-rp-set-priority

**Overview** Use this command to ignore the RP-SET priority value, and use only the hashing mechanism for RP selection.

Use the **no** variant of this command to disable this setting.

**Syntax** `ipv6 pim ignore-rp-set-priority`  
`no ipv6 pim ignore-rp-set-priority`

**Mode** Global Configuration

**Usage** This command is used to inter-operate with older Cisco IOS versions.

**Example** To enable this option, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim ignore-rp-set-priority
```

To disable this option again, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim ignore-rp-set-priority
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2



# ipv6 pim jp-timer

**Overview** Use this command to set the PIM-SMv6 join/prune timer. Note that the value set by the join/prune timer is the value that the device puts into the holdtime field of the join/prune packets it sends to its neighbors.

Use the **no** variant of this command to return the PIM-SMv6 join/prune timer to its default value of 210 seconds.

**Syntax** `ipv6 pim jp-timer <1-65535>`  
`no ipv6 pim jp-timer [<1-65535>]`

| Parameter | Description                                                             |
|-----------|-------------------------------------------------------------------------|
| <1-65535> | Specifies the Join/Prune timer value. The default value is 210 seconds. |

**Default** The default PIM-SMv6 join/prune timer value is 210 seconds.

**Mode** Global Configuration

**Example** To change the join/prune timer to 300 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim jp-timer 300
```

To return the join/prune timer to its default value, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim jp-timer
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim register-rate-limit

**Overview** Use this command to configure the rate of register packets sent by this DR, in units of packets per second. The configured rate is per (S, G) state, and is not a system wide rate.

Use the **no** variant of this command to remove the limit.

**Syntax** `ipv6 pim register-rate-limit <1-65535>`  
`no ipv6 pim register-rate-limit`

| Parameter | Description                                                          |
|-----------|----------------------------------------------------------------------|
| <1-65535> | Specifies the maximum number of packets that can be sent per second. |

**Mode** Global Configuration

**Default** The default is 0, which means no rate limit.

**Examples** To set the rate limit to 3444 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim register-rate-limit 3444
```

To remove the rate limit, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim register-rate-limit
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim register-rp-reachability

**Overview** Use this command to enable the RP reachability check for PIMv6 Register processing at the DR. The default setting is no checking for RP-reachability.

Use the **no** variant of this command to disable this processing.

**Syntax** `ipv6 pim register-rp-reachability`  
`no ipv6 pim register-rp-reachability`

**Default** This command is disabled; by default, there is no checking for RP-reachability.

**Mode** Global Configuration

**Examples** To check for RP reachability, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim register-rp-reachability
```

To stop checking for RP reachability, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim register-rp-reachability
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim register-source

**Overview** Use this command to configure the source IPv6 address of register packets sent by this DR, overriding the default source IPv6 address, which is the IPv6 address of the RPF interface toward the source host.

Use the **no** variant of this command to remove the IPv6 source address of Register packets sent by this DR, reverting back to use the default IPv6 source address that is the address of the RPF interface toward the source host.

**Syntax** `ipv6 pim register-source [<source-IPv6-address>|<interface>]`  
`no ipv6 pim register-source`

| Parameter                                | Description                                                                                       |
|------------------------------------------|---------------------------------------------------------------------------------------------------|
| <code>&lt;source-IPv6-address&gt;</code> | The IPv6 address, entered in the form X:X::X:X, to be used as the source of the register packets. |
| <code>&lt;interface&gt;</code>           | The name of the interface to be used as the source of the register packets.                       |

**Mode** Global Configuration

**Usage** The configured address must be a reachable address to be used by the RP to send corresponding Register-Stop messages in response. It is normally the local loopback IPv6 interface address, but can also be a physical IPv6 address. This IPv6 address must be advertised by unicast routing protocols on the DR. The configured interface does not have to be PIM-SMv6 enabled.

**Mode** Global Configuration

**Examples** To configure the register source as 3ffe::24:2, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim register-source 3ffe::24:2
```

To configure the register source as eth1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim register-source eth1
```

To change back to the default, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# no ipv6 pim register-source
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim register-suppression

**Overview** Use this command to configure the register-suppression time, in seconds, overriding the default of 60 seconds.

Use the **no** variant of this command to reset the value to its default of 60 seconds.

**Syntax** `ipv6 pim register-suppression <1-65535>`  
`no ipv6 pim register-suppression`

| Parameter | Description                              |
|-----------|------------------------------------------|
| <1-65535> | Register suppression on time in seconds. |

**Mode** Global Configuration

**Default** 60 seconds

**Usage** Configuring this value modifies register-suppression time at the DR. Configuring this value at the RP modifies the RP-keepalive-period value if the [ipv6 pim rp-register-kat](#) command is not used.

**Examples** To change the register-suppression time to 192 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim register-suppression 192
```

To return to the default register-suppression time of 60 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim register-suppression
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim rp-address

**Overview** Use this command to statically configure RP (Rendezvous Point) address for IPv6 multicast groups.

Use the **no** variant of this command to remove a statically configured RP (Rendezvous Point) address for IPv6 multicast groups.

**Syntax** `ipv6 pimv6 rp-address <IPv6-address>[override]`  
`no ipv6 pim rp-address <IPv6-address>[override]`

| Parameter      | Description                                                                                                       |
|----------------|-------------------------------------------------------------------------------------------------------------------|
| <IPv6-address> | Specify the IPv6 address of the Rendezvous Point, entered in the form X:X::X:X.                                   |
| override       | Specify this optional parameter keyword to enable any statically defined RPs to override dynamically learned RPs. |

**Mode** Global Configuration

**Usage notes** The AlliedWare Plus™ PIM-SMv6 implementation supports multiple static RPs. It also supports usage of static RPs and the BSR mechanism simultaneously. This command is used to statically configure the RP address for IPv6 multicast groups.

You need to understand the following information before using this command:

If the RP address that is configured by the BSR, and the RP-address that is configured statically, are both available for a group range, then the RP address configured through BSR is chosen over the statically configured RP address.

If multiple static RPs are available for a group range, then one with the highest IPv6 address is chosen.

After configuration, the RP address is inserted into a static RP group tree based on the configured group ranges. For each group range, multiple static RPs are maintained in a list. This list is sorted in a descending order of IPv6 addresses. When selecting static RPs for a group range, the first element (which is the static RP with highest IPv6 address) is chosen.

RP address deletion is handled by removing the static RP from all the existing group ranges and recalculating the RPs for existing TIB states if required.

Group mode and RP address mappings learned through BSR take precedence over mappings statistically defined by this command. Commands with the **override** parameter take precedence over dynamically learned mappings.

**Related commands** [ipv6 pim rp-candidate](#)  
[ipv6 pim rp-register-kat](#)

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim rp-candidate

**Overview** Use this command to make the device an RP (Rendezvous Point) candidate, using the IPv6 address of the specified interface.

Use the **no** variant of this command to stop the device from being an RP candidate.

**Syntax** `ipv6 pim rp-candidate <interface> [priority <priority>|interval <interval>]`  
`no ipv6 pim rp-candidate [<interface>]`

| Parameter              | Description                                                                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface>            | The interface name.                                                                                                                                           |
| priority<br><priority> | The RP candidate priority for this interface on this device, from 0 to 255. The lower the priority value, the more likely this candidate is to become the RP. |
| interval<br><interval> | The advertisement interval, from 1 to 16383 seconds.                                                                                                          |

**Default** The priority value for a candidate RP is 192 by default until specified using the **priority** parameter.

**Mode** Global Configuration

**Usage notes** Note that issuing the command **ipv6 pim rp-candidate <interface>** without optional **priority**, **interval**, or **group-list** parameters will configure the candidate RP with a priority value of 192.

**Examples** To specify a priority of 3, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim rp-candidate eth1 priority 3
```

To stop the device from being an RP candidate on eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim rp-candidate eth1
```

**Related commands** [ipv6 pim rp-address](#)  
[ipv6 pim rp-register-kat](#)

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2



# ipv6 pim rp embedded

**Overview** Use this command to configure and enable embedded RP (Rendezvous Point) in PIM-SMv6.

This command only applies to the embedded RP group range **ff7x::/12** and **fffx::/12**.

Use the **no** variant of this command to disable embedded RP support. Since embedded RP support is enabled by default, use the **no** variant of this command to disable the default.

**Syntax** `ipv6 pim rp embedded`  
`no ipv6 pim rp embedded`

**Mode** Global Configuration

**Default** Enabled

**Examples** The following example re-enables embedded RP support, the default state in PIM-SMv6:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim rp embedded
```

The following example disables embedded RP support, which is enabled by default in PIM-SMv6:

```
awplus# configure terminal
awplus(config)# no ipv6 pim rp embedded
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim rp-register-kat

**Overview** Use this command to configure the Keep Alive Time (KAT) for (S,G) states at the RP (Rendezvous Point) to monitor PIM-SMv6 Register packets.

Use the **no** variant of this command to return the PIM-SMv6 KAT timer to its default value of 210 seconds.

**Syntax** `ipv6 pim rp-register-kat <1-65535>`  
`no ipv6 pim rp-register-kat`

| Parameter | Description                                                         |
|-----------|---------------------------------------------------------------------|
| <1-65536> | Specify the KAT timer in seconds. The default value is 210 seconds. |

**Mode** Global Configuration

**Default** The default PIM-SMv6 KAT timer value is 210 seconds.

**Examples** To change the KAT timer to 3454 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim rp-register-kat 3454
```

To return the KAT timer to its default setting, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim rp-register-kat
```

**Related commands** [ipv6 pim rp-address](#)  
[ipv6 pim rp-candidate](#)

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim sparse-mode

**Overview** Use this command to enable PIM-SMv6 on an interface.  
Use the **no** variant of this command to disable PIM-SMv6 on an interface.

**Syntax** `ipv6 pim sparse-mode`  
`no ipv6 pim sparse-mode`

**Mode** Interface Configuration for an Eth or PPP interface.

**Examples** To enable PIM-SMv6 on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim sparse-mode
```

To disable PIM-SMv6 on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 pim sparse-mode
```

To enable PIM-SMv6 on ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface ppp0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim sparse-mode
```

# ipv6 pim sparse-mode passive

**Overview** Use this command to enable and disable PIM-SMv6 passive mode operation for local members on an interface.

Use the **no** variant of this command to disable PIM-SMv6 passive mode operation for local members on an interface.

**Syntax** `ipv6 pim sparse-mode passive`  
`no ipv6 pim sparse-mode passive`

**Mode** Interface Configuration for an Eth or PPP interface.

**Usage** Passive mode essentially stops PIM-SMv6 transactions on the interface, allowing only the MLD mechanism to be active.

**Examples** To enable passive mode on eth1, use the commands

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim sparse-mode passive
```

To disable passive mode on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 pim sparse-mode passive
```

To enable passive mode on ppp0, use the commands

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface ppp0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim sparse-mode passive
```

# ipv6 pim spt-threshold

**Overview** This command turns on the ability for the last-hop PIM-SMv6 router to switch to SPT (shortest-path tree).

The **no** variant of this command turns off the ability for the last-hop PIM-SMv6 router to switch to SPT.

**NOTE:** *The switching to SPT happens either at the receiving of the first data packet, or not at all; it is not rate-based.*

**Syntax** `ipv6 pim spt-threshold`  
`no ipv6 pim spt-threshold`

**Mode** Global Configuration

**Examples** To enable the last-hop PIM-SMv6 router to switch to SPT, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 pim spt-threshold
```

To stop the last-hop PIM-SMv6 router from being able to switch to SPT, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim spt-threshold
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim ssm

**Overview** Use this command to define the Source Specific Multicast (SSM) range of IPv6 multicast addresses. PIM-SMv6 routers will only install (S,G) entries for multicast groups (addresses) residing in the SSM range.

Use the **no** variant of this command to disable the SSM range.

**Syntax** `ipv6 pim ssm default`  
`no ipv6 pim ssm`

| Parameter | Description                         |
|-----------|-------------------------------------|
| default   | Use FF3x::/32 as the range for SSM. |

**Default** Disabled

**Mode** Global Configuration

**Usage** Any (\*,G) or (S,G,rpt) joins received for multicast groups (addresses) within the range are not installed in PIM-SMv6 mroute table.

**Examples** To use the default address range for PIM-SSM, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 pim ssm default
```

To disable PIM-SSM, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 pim ssm
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# ipv6 pim unicast-bsm

**Overview** Use this command to enable support for the sending and receiving of unicast Bootstrap Messages (BSM) on an interface.

Use the **no** variant of this command to disable the sending and receiving of unicast BSM on an interface.

**Syntax** `ipv6 pim unicast-bsm`  
`no ipv6 pim unicast-bsm`

**Mode** Interface Configuration for an Eth or PPP interface.

**Default** Unicast BSM is disabled by default on an interface.

**Usage** This command provides backward compatibility with older versions of the Bootstrap Router (BSR) specification, which directs unicast BSM to refresh the state of new or restarting neighbors. The current BSR specification defines a No Forward BSM to achieve the same result.

**Examples** To enable BSM messages on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface eth1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 pim unicast-bsm
```

To disable BSM messages on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no ipv6 pim unicast-bsm
```

# service pim6

**Overview** Use this command to enable IPv6 PIM sparse mode services.  
Use the **no** version of the command to disable unused IPv6 PIM sparse mode services.

**Syntax** `service pim6`  
`no service pim6`

**Default** Enabled

**Mode** Global Configuration

**Usage notes** Sometimes it may be desirable to disable unused services, in order to reduce memory use.  
Disabling the PIM services will only take effect after you save the configuration and restart the device.

**Example** To disable the IPv6 PIM sparse mode service, use the commands:

```
awplus# configure terminal
awplus(config)# no service pim6
```

**Output** Figure 32-2: Example output from **no service pim6**

```
awplus(config)#no service pim6
% Save the config and restart the device for this change to take
effect
```

**Command changes** Version 5.5.0-0.1: command added



# show debugging ipv6 pim sparse-mode

**Overview** Use this command to see what debugging is turned on for PIM-SMv6.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show debugging ipv6 pim sparse-mode`

**Mode** User Exec and Privileged Exec

**Example** To display PIM-SMv6 debugging settings, use the command:

```
awplus# show debugging ipv6 pim sparse-mode
```

Figure 32-3: Example output from the **show debugging ipv6 pim sparse-mode** command

```
awplus#show debugging ipv6 pim sparse-mode
Debugging status:
 PIM event debugging is on
 PIM MFC debugging is on
 PIM state debugging is on
 PIM packet debugging is on
 PIM Hello HT timer debugging is on
 PIM Hello NLT timer debugging is on
 PIM Hello THT timer debugging is on
 PIM Join/Prune JT timer debugging is on
 PIM Join/Prune ET timer debugging is on
 PIM Join/Prune PPT timer debugging is on
 PIM Join/Prune KAT timer debugging is on
 PIM Join/Prune OT timer debugging is on
 PIM Assert AT timer debugging is on
 PIM Register RST timer debugging is on
 PIM Bootstrap BST timer debugging is on
 PIM Bootstrap CRP timer debugging is on
```

**Related commands** [debug ipv6 pim sparse-mode](#)  
[undebug ipv6 pim sparse-mode](#)

# show ipv6 pim sparse-mode bsr-router

**Overview** Use this command to show the PIM-SMv6 Bootstrap Router (BSR) IPv6 address.  
For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show ipv6 pim sparse-mode bsr-router`

**Mode** User Exec and Privileged Exec

**Example** To display the BSR IPv6 address, use the command:  
`awplus# show ipv6 pim sparse-mode bsr-router`

**Output** Figure 32-4: Example output from the **show ipv6 pim sparse-mode bsr-router** command

```
awplus#show ipv6 pim sparse-mode bsr-router
PIM6v2 Bootstrap information
 BSR address: 2001:203::213 (?)
 Uptime: 00:36:25, BSR Priority: 64, Hash mask length: 126
 Expires: 00:01:46
 Role: Candidate BSR
 State: Candidate BSR

 Candidate RP: 2001:5::211(eth1)
 Advertisement interval 60 seconds
 Next C-RP advertisement in 00:00:43
```

**Related commands** [show ipv6 pim sparse-mode rp mapping](#)  
[show ipv6 pim sparse-mode neighbor](#)

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 pim sparse-mode interface

**Overview** Use this command to show PIM-SMv6 interface information.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show ipv6 pim sparse-mode interface [detail]`

| Parameter | Description                |
|-----------|----------------------------|
| detail    | Show detailed information. |

**Mode** User Exec and Privileged Exec

**Examples** To display information about all PIM-SMv6 interfaces, use the command:

```
awplus# show ipv6 pim sparse-mode interface
```

**Output** Figure 32-5: Example output from the **show ipv6 pim sparse-mode interface** command

|                                            |          |                            |       |          |
|--------------------------------------------|----------|----------------------------|-------|----------|
| awplus#show ipv6 pim sparse-mode interface |          |                            |       |          |
| Interface                                  | VIFindex | Ver/                       | Nbr   | DR       |
|                                            |          | Mode                       | Count | Priority |
| eth1                                       | 0        | v2/S                       | 2     | 1        |
| Address                                    |          | : fe80::207:e9ff:fe02:81d  |       |          |
| Global Address                             |          | : 3ffe:192:168:1::53       |       |          |
| DR                                         |          | : fe80::20e:cff:fe01:facc  |       |          |
| eth2                                       | 2        | v2/S                       | 2     | 1        |
| Address                                    |          | : fe80::207:e9ff:fe02:21a2 |       |          |
| Global Address                             |          | : 3ffe:192:168:10::53      |       |          |
| DR                                         |          | : this system              |       |          |

**Table 1:** Parameters in the output from the **show ipv6 pim sparse-mode interface** command

| Parameters | Description                                   |
|------------|-----------------------------------------------|
| Address    | Primary PIM-SMv6 address.                     |
| Interface  | Name of the PIM-SMv6 interface.               |
| VIF Index  | The Virtual Interface index of the interface. |
| Ver/Mode   | PIMv6 version/Sparse mode.                    |
| Nbr Count  | Neighbor count of the PIM-SMv6 interface.     |

**Table 1:** Parameters in the output from the **show ipv6 pim sparse-mode interface** command (cont.)

| Parameters  | Description                                |
|-------------|--------------------------------------------|
| DR Priority | Designated Router priority.                |
| DR          | The IPv6 address of the Designated Router. |

**Related commands**

- [ipv6 pim sparse-mode](#)
- [show ipv6 pim sparse-mode rp mapping](#)
- [show ipv6 pim sparse-mode neighbor](#)

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 pim sparse-mode interface detail

**Overview** Use this command to show detailed PIM-SMv6 information for all PIM-SMv6 configured interfaces.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show ipv6 pim sparse-mode interface detail`

**Mode** User Exec and Privileged Exec

**Example** To show detailed PIM-SMv6 information for all PIM-SMv6 configured interfaces, use the command:

```
awplus# show ipv6 pim sparse-mode interface detail
```

**Output** Figure 32-6: Example output from the **show ipv6 pim sparse-mode interface detail** command

```
awplus#show ipv6 pim sparse-mode interface detail
eth1 (vif 0)
 Address fe80::207:e9ff:fe02:81d, DR fe80::20e:cff:fe01:facc
 Hello period 30 seconds, Next Hello in 21 seconds
 Triggered Hello period 5 seconds
 Secondary addresses:
 3ffe:192:168:1::53
 Neighbors:
 fe80::202:b3ff:fed4:69fe
 fe80::20e:cff:fe01:facc

eth2 (vif 2):
 Address fe80::207:e9ff:fe02:21a2, DR fe80::207:e9ff:fe02:21a2
 Hello period 30 seconds, Next Hello in 20 seconds
 Triggered Hello period 5 seconds
 Secondary addresses:
 3ffe:192:168:10::53
 Neighbors:
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 pim sparse-mode local-members

**Overview** Use this command to show detailed local member information on an interface configured for PIM-SMv6. If you do not specify an interface then detailed local member information is shown for all interfaces configured for PIM-SMv6.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show ipv6 pim sparse-mode local-members [<interface>]`

| Parameter   | Description                                |
|-------------|--------------------------------------------|
| <interface> | An interface to display information about. |

**Mode** User Exec and Privileged Exec

**Example** To show detailed PIM-SMv6 information for all PIM-SMv6 configured interfaces, use the command:

```
awplus# show ipv6 pim sparse-mode local-members
```

**Output** Figure 32-7: Example output from the **show ipv6 pim sparse-mode local-members** command

```
awplus#show ipv6 pim sparse-mode local-members
PIM Local membership information

eth1:

 (*, ff02::1:ff6b:4783) : Include

eth2:

 (*, ff0e:1::4) : Include
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 pim sparse-mode mroute

**Overview** Use this command to display the IPv6 multicast routing table, or the IPv6 multicast routing table based on the specified IPv6 address or addresses.

Two group IPv6 addresses cannot be entered simultaneously; two source IPv6 addresses cannot be entered simultaneously.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax**

```
show ipv6 pim sparse-mode mroute
show ipv6 pim sparse-mode mroute <group-IPv6-address>
show ipv6 pim sparse-mode mroute <source-IPv6-address>
show ipv6 pim sparse-mode mroute <group-IPv6-address>
<source-IPv6-address>
show ipv6 pim sparse-mode mroute <source-IPv6-address>
<group-IPv6-address>
show ipv6 pim sparse-mode mroute brief
```

| Parameter             | Description                                                                                                                                                             |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <group-IPv6-address>  | Group IPv6 address, entered in the form X:X::X:X. Based on the group and source IPv6 address, the output is the selected route if present in the multicast route tree.  |
| <source-IPv6-address> | Source IPv6 address, entered in the form X:X::X:X. Based on the source and group IPv6 address, the output is the selected route if present in the multicast route tree. |
| brief                 | Brief display.                                                                                                                                                          |

**Mode** User Exec and Privileged Exec

**Usage notes** Note that when a feature license is enabled, the output for the [show ipv6 pim sparse-mode mroute](#) command will only show 100 interfaces because of the terminal display width limit. Use the [show ipv6 pim sparse-mode mroute detail](#) command to display detailed entries of the IPv6 multicast routing table.

**Examples**

```
awplus# show ipv6 pim sparse-mode mroute
awplus# show ipv6 pim sparse-mode mroute 2001:db8::
awplus# show ipv6 pim sparse-mode mroute 2001:db8:: 2002:db8::
awplus# show ipv6 pim sparse-mode mroute brief
```

**Output** Figure 32-8: Example output from the **show ipv6 pim sparse-mode mroute** command

```
awplus#show ipv6 pim sparse-mode mroute
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0(*,G) Entries: 0
(S,G) Entries: 2
(S,G,rpt) Entries: 2
FCR Entries: 0(2001:db8:ffff::1, ff08::1)
RPF nbr: fe80::b:10:0:1
RPF idx: eth1
SPT bit: 1
Upstream State: JOINED
 Local 0
 Joined 1
 Asserted Winner 0
 Asserted Loser 0
 Outgoing 1(2001:db8:ffff::1, ff08::1, rpt)
RP: ::
RPF nbr: fe80::b:10:0:1
RPF idx: eth1
Upstream State: RPT NOT JOINED
 Local 0
 Pruned 0
 Outgoing 0(2001:db8:ffff::1, ff08::2)
RPF nbr: fe80::b:10:0:1
RPF idx: eth1
SPT bit: 1
Upstream State: JOINED
 Local 0
 Joined 1
 Asserted Winner 0
 Asserted Loser 0
 Outgoing 1
```

Figure 32-9: Example output from the **show ipv6 pim sparse-mode mroute brief** command

```
awplus#show ipv6 pim sparse-mode mroute brief
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 0
(S,G) Entries: 2
(S,G,rpt) Entries: 2
FCR Entries: 0
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2



# show ipv6 pim sparse-mode mroute detail

**Overview** Use this command to display detailed entries of the IPv6 multicast routing table, or detailed entries of the IPv6 multicast routing table based on the specified IPv6 address or addresses.

Two group IPv6 addresses cannot be used simultaneously; two IPv6 source addresses cannot be used simultaneously.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax**

```
show ipv6 pim sparse-mode mroute
[<group-IPv6-address>|<source-IPv6-address>] detail

show ipv6 pim sparse-mode mroute [<group-IPv6-address>
<source-IPv6-address>] detail

show ipv6 pim sparse-mode mroute [<source-IPv6-address>
<group-IPv6-address>] detail
```

| Parameter             | Description                                                                                                  |
|-----------------------|--------------------------------------------------------------------------------------------------------------|
| <group-IPv6-address>  | Group IPv6 address, entered in the form X:X::X:X. Output is all multicast entries belonging to that group.   |
| <source-IPv6-address> | Source IPv6 address, entered in the form X:X::X:X. Output is all multicast entries belonging to that source. |
| detail                | Show detailed information.                                                                                   |

**Mode** User Exec and Privileged Exec

**Usage notes** Based on the group and source IPv6 address, the output is the selected route if present in the multicast route tree.

**Examples**

```
awplus# show ipv6 pim sparse-mode mroute detail
awplus# show ipv6 pim sparse-mode mroute 2001:db8:: detail
awplus# show ipv6 pim sparse-mode mroute 2001:db8:: 2002:db8::
detail
```

**Output** Figure 32-10: Example output from the **show ipv6 pim sparse-mode mroute detail** command

```
awplus#show ipv6 pim sparse-mode mroute detail
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, ff13::10) Uptime: 00:00:09
RP: ::, RPF nbr: None, RPF idx: None
Upstream:
 State: JOINED, SPT Switch: Enabled, JT: off
 Macro state: Join Desired,
Downstream:
 eth1:
 State: NO INFO, ET: off, PPT: off
 Assert State: NO INFO, AT: off
 Winner: ::, Metric: 42949672951, Pref: 42949672951, RPT bit: on
 Macro state: Could Assert, Assert Track
Local Olist:
 eth2
FCR:
```

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 pim sparse-mode neighbor

**Overview** Use this command to show the PIM-SMv6 neighbor information.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show ipv6 pim sparse-mode neighbor [<interface>]  
[<IPv6-address>] [detail]`

| Parameter      | Description                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------|
| <interface>    | Interface name. Show neighbors on an interface.                                                          |
| <IPv6-address> | Show neighbors with a particular address on an interface. The IPv6 address entered in the form X:X::X:X. |
| detail         | Show detailed information.                                                                               |

**Mode** User Exec and Privileged Exec

**Examples** `awplus# show ipv6 pim sparse-mode neighbor`  
`awplus# show ipv6 pim sparse-mode neighbor eth1 detail`

**Output** Figure 32-11: Example output from the **show ipv6 pim sparse-mode neighbor** command

```
awplus#show ipv6 pim sparse-mode neighbor
```

| Neighbor Address         | Interface | Uptime/Expires    | DR       |
|--------------------------|-----------|-------------------|----------|
|                          |           |                   | Pri/Mode |
| fe80::202:b3ff:fed4:69fe | eth1      | 05:33:52/00:01:41 | 1 /      |
| fe80::20e:cff:fe01:facc  | eth2      | 05:33:53/00:01:26 | 1 / DR   |

Figure 32-12: Example output from the **show ipv6 pim sparse-mode neighbor interface detail** command

```
awplus#show ipv6 pim sparse-mode neighbor detail
```

|                                                                   |
|-------------------------------------------------------------------|
| Nbr fe80::211:11ff:fe44:4cd8 (eth1), DR                           |
| Expires in 64 seconds, uptime 00:00:53                            |
| Holdtime: 70 secs, T-bit: off, lan delay: 1, Override interval: 3 |
| DR priority: 100, Gen ID: 1080091886,                             |
| Secondary addresses:                                              |
| 3ffe:10:10:10:3::180                                              |

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 pim sparse-mode nexthop

**Overview** Use this command to see the next hop information as used by PIM-SMv6.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show ipv6 pim sparse-mode nexthop`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ipv6 pim sparse-mode nexthop`

**Output** Figure 32-13: Example output from the **show ipv6 pim sparse-mode nexthop** command

|                                                     |      |                |                         |                    |                 |        |      |        |
|-----------------------------------------------------|------|----------------|-------------------------|--------------------|-----------------|--------|------|--------|
| awplus#show ipv6 pim sparse-mode nexthop            |      |                |                         |                    |                 |        |      |        |
| Flags: N = New, R = RP, S = Source, U = Unreachable |      |                |                         |                    |                 |        |      |        |
| Destination                                         | Type | Nexthop<br>Num | Nexthop<br>Addr         | Nexthop<br>Ifindex | Nexthop<br>Name | Metric | Pref | Refcnt |
| 3ffe:10:10:5::153                                   | .RS. | 1              | fe80::20e:cff:fe01:facc | 2                  | 30              | 110    | 1    |        |

**Table 2:** Parameters in output of the **show ipv6 pim sparse-mode nexthop** command

| Parameter       | Description                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------|
| Destination     | The destination address for which PIM-SMv6 requires next hop information.                                    |
| Type            | The type of destination, as indicated by the Flags description. N = New, R= RP, S = Source, U = Unreachable. |
| Nexthop Num     | The number of next hops to the destination. PIM-SMv6 always uses only 1 next hop.                            |
| Nexthop Addr    | The address of the primary next hop gateway.                                                                 |
| Nexthop IfIndex | The interface on which the next hop gateway can be reached.                                                  |
| Nexthop Name    | The name of next hop interface.                                                                              |
| Metric          | The metric of the route towards the destination.                                                             |
| Preference      | The preference of the route towards destination.                                                             |
| Refcnt          | Only used for debugging.                                                                                     |

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 pim sparse-mode rp-hash

**Overview** Use this command to display the Rendezvous Point (RP) to be chosen based on the IPv6 group address selected.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 pim sparse-mode rp-hash <IPv6-group-addr>`

| Parameter                            | Description                                                               |
|--------------------------------------|---------------------------------------------------------------------------|
| <code>&lt;IPv6-group-addr&gt;</code> | The IPv6 group address used to find the RP, entered in the form X:X::X:X. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ipv6 pim sparse-mode rp-hash ff04:10`

**Output** Figure 32-14: Output from the **show ipv6 pim sparse-mode rp-hash** command:

```
awplus#show ipv6 pim sparse-mode rp-hash ff04::10
RP: 3ffe:10:10:5::153
Info source: 3ffe:10:10:5::153, via bootstrap
```

**Related commands** [show ipv6 pim sparse-mode rp mapping](#)

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 pim sparse-mode rp mapping

**Overview** Use this command to show group-to-RP (Rendezvous Point) mappings, and the RP set.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show ipv6 pim sparse-mode rp mapping`

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ipv6 pim sparse-mode rp mapping`

**Output** Figure 32-15: Output from the **show ipv6 pim sparse-mode rp mapping** command

```
awplus#show ipv6 pim sparse-mode rp mapping
PIM Group-to-RP Mappings
Group(s): ff00::/8
 RP: 3ffe:10:10:5::153
 Info source: 3ffe:10:10:5::153, via bootstrap, priority 192
 Uptime: 05:36:40
```

**Related commands** [show ipv6 pim sparse-mode rp-hash](#)

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# show ipv6 pim sparse-mode rp nexthop

**Overview** Use this command to display the RP (Rendezvous Point) next hop information used by PIM-SMv6.

For information on filtering and saving command output, see the [“Getting\\_Started with AlliedWare Plus” Feature Overview and Configuration\\_Guide](#).

**Syntax** `show ipv6 pim sparse-mode rp nexthop <RP-group-addr>`

| Parameter       | Description                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------|
| <RP-group-addr> | Specify the RP group address used to display next hop RP information, entered in the form X:X::X:X. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ipv6 pim sparse-mode rp nexthop 3ffe:10:10:5::153`

**Output** Figure 32-16: Example output from the **show ipv6 pim sparse-mode rp nexthop** command

|                                                               |      |             |                         |                 |              |        |      |        |  |
|---------------------------------------------------------------|------|-------------|-------------------------|-----------------|--------------|--------|------|--------|--|
| awplus#show ipv6 pim sparse-mode rp nexthop 3ffe:10:10:5::153 |      |             |                         |                 |              |        |      |        |  |
| Flags: N = New, R = RP, S = Source, U = Unreachable           |      |             |                         |                 |              |        |      |        |  |
| Destination                                                   | Type | Nexthop Num | Nexthop Addr            | Nexthop Ifindex | Nexthop Name | Metric | Pref | Refcnt |  |
| 3ffe:10:10:5::153                                             | .RS. | 1           | fe80::20e:cff:fe01:facc | 2               | 30           | 110    | 1    |        |  |

**Table 3:** Parameters in output of the **show ipv6 pim sparse-mode rp nexthop** command

| Parameter       | Description                                                                                                  |
|-----------------|--------------------------------------------------------------------------------------------------------------|
| Destination     | The destination address for which PIM-SMv6 requires next hop information.                                    |
| Type            | The type of destination, as indicated by the Flags description. N = New, R= RP, S = Source, U = Unreachable. |
| Nexthop Num     | The number of next hops to the destination. PIM-SMv6 always uses only 1 next hop.                            |
| Nexthop Addr    | The address of the primary next hop gateway.                                                                 |
| Nexthop IfIndex | The interface on which the next hop gateway can be reached.                                                  |
| Nexthop Name    | The name of next hop interface.                                                                              |



**Table 3:** Parameters in output of the **show ipv6 pim sparse-mode rp nexthop** command (cont.)

| Parameter  | Description                                      |
|------------|--------------------------------------------------|
| Metric     | The metric of the route towards the destination. |
| Preference | The preference of the route towards destination. |
| Refcnt     | Only used for debugging.                         |

**Command changes** Version 5.5.4-2.3: VRF-lite support added for x530, x530L, x540L, x930, x950, SBx8100, SBx908 GEN2

# undebug all ipv6 pim sparse-mode

**Overview** Use this command to disable all PIM-SMv6 debugging.

**Syntax** `undebug all ipv6 pim sparse-mode`

**Mode** Privileged Exec

**Example** `awplus# undebug all ipv6 pim sparse-mode`

**Related commands** [debug ipv6 pim sparse-mode](#)

# undebg ipv6 pim sparse-mode

**Overview** Use this command to deactivate PIM-SMv6 debugging. Note that this command is an alias of the no variant of the [debug ipv6 pim sparse-mode](#) command.

**Syntax** undebg ipv6 pim sparse-mode [all] [events] [mfc] [mib] [nexthop] [nsm] [state] [timer]

| Parameter | Description                                                                     |
|-----------|---------------------------------------------------------------------------------|
| all       | Deactivates all PIM-SMv6 debugging.                                             |
| events    | Deactivates debug printing of PIM-SMv6 events.                                  |
| mfc       | Deactivates debug printing of MFC (Multicast Forwarding Cache).                 |
| mib       | Deactivates debug printing of PIM-SMv6 MIBs.                                    |
| nexthop   | Deactivates debug printing of PIM-SMv6 next hop communications.                 |
| nsm       | Deactivates debugging of PIM-SMv6 NSM (Network Services Module) communications. |
| state     | Deactivates debug printing of state transition on all PIM-SMv6 FSMs.            |
| timer     | Deactivates debug printing of PIM-SMv6 timers.                                  |

**Mode** Privileged Exec and Global Configuration

**Example**

```
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# undebg ipv6 pim sparse-mode all
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# undebg ipv6 pim sparse-mode events
awplus# configure terminal
awplus(config)# terminal monitor
awplus(config)# undebg ipv6 pim sparse-mode nexthop
```

**Validation  
Output**

Figure 32-17: Example output from the **show debugging ipv6 pim sparse-mode** command after issuing the **undebg ipv6 pim sparse-mode all** command

```
awplus#undebg ipv6 pim sparse-mode all
awplus#show debugging ipv6 pim sparse-mode
PIM-SMv6 debugging status:
 PIM event debugging is off
 PIM MFC debugging is off
 PIM state debugging is off
 PIM packet debugging is off
 PIM Hello HT timer debugging is off
 PIM Hello NLT timer debugging is off
 PIM Hello THT timer debugging is off
 PIM Join/Prune JT timer debugging is off
 PIM Join/Prune ET timer debugging is off
 PIM Join/Prune PPT timer debugging is off
 PIM Join/Prune KAT timer debugging is off
 PIM Join/Prune OT timer debugging is off
 PIM Assert AT timer debugging is off
 PIM Register RST timer debugging is off
 PIM Bootstrap BST timer debugging is off
 PIM Bootstrap CRP timer debugging is off
 PIM mib debugging is off
 PIM nsm debugging is off
 PIM nexthop debugging is off
```

**Related  
commands**

[debug ipv6 pim sparse-mode](#)  
[show debugging ipv6 pim sparse-mode](#)  
[undebg all ipv6 pim sparse-mode](#)

# Part 5: Access and Security

# 33

# Traffic Control Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure traffic control. For more information, see the [Traffic Control Feature Overview and Configuration Guide](#).

- Command List**
- ["class \(htb\)"](#) on page 1532
  - ["class \(priority\)"](#) on page 1534
  - ["class \(wrr\)"](#) on page 1536
  - ["debug traffic-control"](#) on page 1538
  - ["interface \(traffic-control\)"](#) on page 1539
  - ["interface dynamic-virtual-bandwidth"](#) on page 1541
  - ["l3-filtering enable"](#) on page 1543
  - ["move rule \(traffic-control\)"](#) on page 1544
  - ["policy \(traffic-control\)"](#) on page 1545
  - ["red-curve"](#) on page 1547
  - ["rule \(traffic-control\)"](#) on page 1549
  - ["show debugging traffic-control"](#) on page 1551
  - ["show running-config traffic-control"](#) on page 1552
  - ["show traffic-control counters"](#) on page 1553
  - ["show traffic-control interface"](#) on page 1555
  - ["show traffic-control policy"](#) on page 1556
  - ["show traffic-control red-curve"](#) on page 1558
  - ["show traffic-control rule config-check"](#) on page 1560
  - ["show traffic-control rule"](#) on page 1561

- [“show traffic-control”](#) on page 1562
- [“sub-class \(htb\)”](#) on page 1563
- [“sub-class \(priority\)”](#) on page 1565
- [“sub-class \(wrr\)”](#) on page 1567
- [“sub-sub-class \(htb\)”](#) on page 1569
- [“sub-sub-class \(priority\)”](#) on page 1571
- [“sub-sub-class \(wrr\)”](#) on page 1573
- [“traffic-control enable”](#) on page 1575
- [“traffic-control”](#) on page 1576

# class (htb)

**Overview** Use this command to configure a hierarchy token bucket (HTB) class within a traffic control policy.

Use the **no** variant of this command to delete an existing class under a current policy.

**Syntax**

```
class <class-name> [cir <committed-rate>] [pir <peak-rate>]
[bc <1-100000000>] [be <1-100000000>] [preference <0-7>]
[queue-length <2-65536>] [set-dscp <dscp-value>] [red-curve
<red-curve-name>]

class <class-name> [cir <committed-rate>] [pir <peak-rate>]
[bc <1-100000000>] [be <1-100000000>] [preference <0-7>]
sub-class-policy htb

no class <class-name>
```

| Parameter                  | Description                                                                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <class-name>               | Name of the class.                                                                                                                                                                         |
| cir <committed-rate>       | Set the Committed Information Rate (CIR) for the queue. This parameter is compulsory when creating a new class. When editing an existing class, this parameter is optional.                |
| pir <peak-rate>            | Set the Peak Information Rate (PIR) for the queue. This is the rate of the queue under peak conditions. Specified in kbit/mbit/gbit per second, in the range 1kbit-100gbit.                |
| bc <1-100000000>           | Set the Committed Burst size (BC). This is the burst allowed above the CIR sent at the PIR rate.                                                                                           |
| be <1-100000000>           | Set the Excess Burst size (BE). This is the burst allowed above the PIR sent at the maximum rate.                                                                                          |
| preference <0-7>           | Set the preference for a class to receive spare bandwidth. Preference for the class to receive spare bandwidth (highest is 7).                                                             |
| queue-length <2-65536>     | Set the maximum queue length.                                                                                                                                                              |
| set-dscp <dscp-value>      | Set the DSCP value to apply to the packets.                                                                                                                                                |
| red-curve <red-curve-name> | Apply a random early discard template with the class (only available on leaf queues when specifying class policy). If the keyword <default> is used then the default RED curve is applied. |
| sub-class-policy           | Specify that the class will contain sub-classes.                                                                                                                                           |
| htb                        | Sub-classes will use the Hierarchy Token Bucket (HTB) queueing discipline.                                                                                                                 |

**Default** BC and BE are assigned suitable values proportional to the CIR and PIR respectively, and are larger than the MTU. The PIR defaults to the CIR. The Preference defaults to 7 and the queue-length defaults to 1000 (if the class is a leaf). If the keyword <default> is used then the default RED curve is applied.



**Mode** Traffic-Control Policy for an HTB policy.

**Usage** If there is already a class in the same level that has the specified name, the command will replace the configuration of the existing class if it does not have any sub-classes.

If a sub-class policy is specified, this command uses the Traffic-Control Class mode to apply it.

**Examples** To configure a leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01 cir 100mbit pir 150mbit
```

To configure a class with a sub-sub-class as the leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01 cir 100mbit pir 150mbit
sub-class-policy htb
awplus(config-tc-class)#sub-class s01 cir 10mbit sub-sub-class
policy htb
awplus(config-tc-subclass)#sub-sub-class ss01 cir 5mbit
queue-length 200 red-curve ss01-red
```

To enter Traffic-Control Class mode for an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#
```

To delete an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#no class c01
```

**Related commands** [policy \(traffic-control\)](#)  
[sub-class \(htb\)](#)  
[traffic-control](#)

# class (priority)

**Overview** Use this command to configure a priority queue class within a traffic control policy.

Use the **no** variant of this command to delete an existing priority class under a current policy.

**Syntax** `class <class-name> [priority-level <0-15>] [max <max-rate>]  
[queue-length <2-65536>] [set-dscp <dscp-value>] [red-curve  
<red-curve-name>]`

`class <class-name> [priority-level <0-15>] sub-class-policy  
{priority|wrr|htb}`

`no class <class-name>`

| Parameter                  | Description                                                                                                                                                                                |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <class-name>               | Name of the class.                                                                                                                                                                         |
| priority-level <0-15>      | Set the priority level (15 is the highest). This parameter is compulsory when creating a new class. When editing an existing class, this parameter is optional.                            |
| max <max-rate>             | Set the maximum traffic rate of the queue (in kbit/mbit/gbit per second, 1kbit-100gbit).                                                                                                   |
| queue-length <2-65535>     | Set the maximum queue length in packets (only available on leaf queues when specifying sub-class policy).                                                                                  |
| set-dscp <dscp-value>      | Set the DSCP value to apply to the packets (only available on leaf queues when specifying sub-class policy).                                                                               |
| red-curve <red-curve-name> | Apply a random early discard template with the class (only available on leaf queues when specifying class policy). If the keyword <default> is used then the default RED curve is applied. |
| sub-class-policy           | Create a sub-class within the policy.                                                                                                                                                      |
| priority                   | Sub-classes use the Priority Queue scheduling algorithm.                                                                                                                                   |
| wrr                        | Sub-classes use the Weighted Round Robin scheduling algorithm.                                                                                                                             |
| htb                        | Sub-classes use the Hierarchy Token Bucket scheduling algorithm.                                                                                                                           |

**Default** No priority class is applied. If the keyword <default> is used then the default RED curve is applied.

**Mode** Traffic Control Policy for a priority policy.

**Usage** If there is already a class in the same level with the specified name, the command will replace the configuration of the existing class if it does not have any sub-classes.

If a sub-class policy is specified, this command uses the Traffic-Control Class mode to apply it.

**Examples** To configure a leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01 priority-level 5
```

To configure a class with a sub-sub-class as the leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01 priority-level 5
sub-class-policy priority
awplus(config-tc-class)#sub-class s01 priority-level 7
sub-sub-class-policy priority
awplus(config-tc-subclass)#sub-sub-class ss01 priority-level 3
max 5mbit queue-length 200 red-curve ss01-red
```

To enter Traffic-Control Class mode for an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#
```

To delete an existing policy class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#no class c01
```

**Related commands**

- [policy \(traffic-control\)](#)
- [sub-class \(htb\)](#)
- [sub-class \(wrr\)](#)
- [traffic-control](#)

## class (wrr)

**Overview** Use this command to configure a Weighted Round-Robin (WRR) class within a traffic control policy.

Use the **no** variant of this command to delete an existing class under a current policy.

**Syntax** `class <class-name> [weight <1-100>] [queue-length <2-65536>]  
[set-dscp <dscp-value>] [red-curve <red-curve-name>]  
class <class-name> [weight <1-100>] sub-class-policy wrr  
no class <class-name>`

| Parameter                  | Description                                                                                                                                                                                                                                                                   |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <class-name>               | Name of the class.                                                                                                                                                                                                                                                            |
| weight <1-100>             | Set the weight. The relative weight is the available bandwidth divided between sibling WRR classes according to the ratio of their configured weights.<br>This parameter is compulsory when creating a new class. When editing an existing class, this parameter is optional. |
| queue-length <2-65536>     | Set the maximum queue length in packets.                                                                                                                                                                                                                                      |
| set-dscp <dscp-value>      | Set the DSCP value to apply to packets.                                                                                                                                                                                                                                       |
| red-curve <red-curve-name> | Apply a random early discard template with the class (only available on leaf queues when specifying class policy). If the keyword <default> is used then the default RED curve is applied.                                                                                    |
| sub-class-policy           | Create a sub-class within the policy.                                                                                                                                                                                                                                         |
| wrr                        | Sub-classes use the Weighted Round Robin queueing algorithm.                                                                                                                                                                                                                  |

**Default** A weighted round-robin class has no DSCP value or sub-class policy. The queue length is 1000 by default. If the keyword <default> is used then the default RED curve is applied.

**Mode** Traffic-Control Policy for a WRR policy.

**Usage** If there is already a class in the same level with the specified name, the command will replace the configuration of the existing class if it does not have any sub-classes.

If a sub-class policy is specified, this command uses the Traffic-Control Class mode to apply it.

**Examples** To configure a leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 wrr
awplus(config-tc-policy)#class c01 weight 50
```

To configure a class with a sub-sub-class as the leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 wrr
awplus(config-tc-policy)#class c01 weight 50 sub-class-policy
wrr
awplus(config-tc-class)#sub-class s01 weight 30 sub-sub-class-
policy wrr
awplus(config-tc-subclass)#sub-sub-class ss01 weight 5
queue-length 200 red-curve ss01-red
```

To enter Traffic-Control Class mode for an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#
```

To delete an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#no class c01
```

**Related  
commands** [traffic-control](#)  
[policy \(traffic-control\)](#)  
[sub-class \(wrr\)](#)

# debug traffic-control

**Overview** Use this command to enable traffic-control debugging. This will cause additional detailed debugging information to be logged and available using the show debugging traffic-control.

Use the **no** variant of this command to disable traffic-control debugging.

**Syntax** debug traffic-control  
no debug traffic-control

**Default** Disabled

**Mode** Privileged Exec

**Examples** To enable traffic control debugging, use the commands:

```
awplus#debug traffic-control
```

To disable traffic control debugging, use the commands:

```
awplus#no debug traffic-control
```

**Related commands** traffic-control  
show debugging traffic-control

# interface (traffic-control)

**Overview** Use this command to configure interface specific parameters for traffic control.

**Syntax** `interface <interface-name> {overhead  
[<overhead-bytes>|ethernet]|virtual-bandwidth  
<bandwidth>|system-bandwidth <system-percentage>}`

| Parameter           | Description                                                                                                                                                   |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface-name>    | Name of interface to configure                                                                                                                                |
| overhead            | Set overhead to add to each packet when calculating the packet size                                                                                           |
| <overhead-bytes>    | Number of bytes to add to the packet for packet size calculations. The range is from 0 to 512 and the default is 0.                                           |
| ethernet            | Setting the overhead to 'ethernet' adds 24 bytes to the packet to account for preamble + CRC + inter-frame gap.                                               |
| virtual-bandwidth   | Specify the virtual-bandwidth of the interface. This is the maximum amount of traffic that traffic control will allow to be sent via the interface..          |
| <bandwidth>         | Value for the virtual bandwidth in kbit, mbit or gbits (for example, 5mbit).                                                                                  |
| system-bandwidth    | Specify the percentage of the interface bandwidth to reserve for system traffic. The default when a traffic control policy is applied to the interface is 5%. |
| <system-percentage> | Percentage of the bandwidth to reserve for system traffic in the range from 1 to 99.                                                                          |

**Default** The default overhead is 0, the default bandwidth is the interface speed if it can be read. It is recommended to always set the virtual bandwidth when using traffic control. The system bandwidth default is 5%.

**Mode** Traffic-Control

**Usage** This command allows configuring traffic control parameters specific to the traffic egress interface.

Note that if you use Vista Manager EX's Auto Traffic Shaping feature, it will dynamically set the virtual bandwidth. In that situation, if you use this command to set the virtual bandwidth, your setting will only apply until Vista Manager EX dynamically overrides it. Your setting also won't be saved in the running config.

See the [interface dynamic-virtual-bandwidth](#) command for more information about the virtual bandwidth when using Auto Traffic Shaping.

**Examples** To rate limit eth1 to 10mbit while taking into account the ethernet framing overhead and reserving only 1% of the bandwidth for system traffic, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#interface eth1 overhead ethernet
virtual-bandwidth 10mbit system-bandwidth 1
```

**Related commands**

- [interface dynamic-virtual-bandwidth](#)
- [show running-config traffic-control](#)
- [show traffic-control interface](#)

**Command changes** Version 5.5.0-1.1: behavior changed when Auto Traffic Shaping is enabled in Vista Manager EX



# interface dynamic-virtual-bandwidth

**Overview** Use this command to set or change the 'initial' virtual bandwidth value when Vista Manager EX has control of the virtual bandwidth on an interface. Vista Manager EX controls virtual bandwidth as part of Auto Traffic Shaping (ATS).

The device will use this command's virtual bandwidth in two situations:

- If you reboot the device, the device uses this virtual bandwidth until Vista Manager EX takes over control of the bandwidth
- It becomes the interface's virtual bandwidth if you turn off Auto Traffic Shaping in Vista Manager EX.

When Auto Traffic Shaping is on, the device does not store the interface's virtual-bandwidth in the device's running-config. This is to prevent Vista Manager EX's dynamic virtual bandwidth values from becoming permanent values.

Use the **no** variant of this command to indicate that Vista Manager EX no longer controls virtual bandwidth on this interface. Using the **no** variant does not change the current virtual-bandwidth value for the interface. If the current virtual-bandwidth value is not the default value, it will display in the device's running-config.

**Syntax** `interface <tunnel-name> dynamic-virtual-bandwidth controller <name> [initial-bandwidth <bandwidth>]`  
`no interface <interface-name> dynamic-virtual-bandwidth`

| Parameter                                        | Description                                                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;tunnel-name&gt;</code>                 | Name of the tunnel to configure                                                                                                                                                                                                                                                                                                        |
| <code>controller &lt;name&gt;</code>             | An identifier for the controller that is controlling the bandwidth. When Vista Manager EX is the controller, it will automatically set this value to 'vista-dynamic-management'. The name may contain alphanumeric, hyphen, underscore, comma, space or square brace characters, with a limit of 64 characters.                        |
| <code>initial-bandwidth &lt;bandwidth&gt;</code> | The value to apply as the interface's virtual-bandwidth when the interface starts up and if you turn ATS off. This value is the maximum amount of traffic that traffic control will allow the device to send via the interface (until the external manager changes it). Specify the value in kbit, mbit or gbits (for example, 5mbit). |

**Default** If you turn on ATS in Vista Manager EX and do not use this command to set the initial bandwidth, then the device uses the virtual-bandwidth value from the command [interface \(traffic-control\)](#).

**Mode** Traffic-Control

**Examples** To set an initial virtual-bandwidth of 10Mbps on tunnel2 when using Auto Traffic Shaping on Vista Manager EX, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#interface tunnel2 dynamic-virtual-bandwidth
controller vista-dynamic-management initial-bandwidth 10mbit
```

**Related commands** [traffic-control](#)  
[show running-config traffic-control](#)  
[show traffic-control interface](#)

**Command changes** Version 5.5.0-1.1: command added

# l3-filtering enable

**Overview** Use this command to enable traffic control for bridged traffic on a bridge interface. Use the **no** variant of this command to disable traffic control for bridged traffic on a bridge interface.

**Syntax** `l3-filtering enable`  
`no l3-filtering enable`

**Default** Traffic control is disabled by default for bridged traffic.

**Mode** Interface mode for a bridge interface

**Usage notes** We do not recommend shaping bridged traffic on firewalls that are running Unified Threat Management (UTM) features, because both Traffic Control and UTM require significant CPU resources.

**Example** To enable traffic control for bridged traffic on br1, use the commands:

```
awplus# configure terminal
awplus(config)# interface br1
awplus(config-if)# l3-filtering enable
```

**Related commands** [traffic-control](#)

**Command changes** Version 5.4.7-0.1: command added. Previously, traffic control was enabled by default on all bridge interfaces.

# move rule (traffic-control)

**Overview** Use this command to change the identification of an existing traffic control rule.

**Syntax** `move rule [<1-65535> to <1-65535>]`

| Parameter | Description                                         |
|-----------|-----------------------------------------------------|
| <1-65535> | Range of the rule ID to move from                   |
| <1-65535> | Range of the destination ID for the rule to move to |

**Default** None

**Mode** Traffic-Control

**Example** To change rule ID 10 to rule ID 25, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#move rule 10 to 25
```

**Related commands**

- [rule \(traffic-control\)](#)
- [traffic-control](#)
- [show traffic-control](#)
- [show traffic-control rule](#)
- [show traffic-control rule config-check](#)

# policy (traffic-control)

**Overview** Use this command to configure a traffic control policy, that can then be used with rules that have been created.

Use the **no** variant of this command to delete an existing policy.

**Syntax** `policy <policy-name> [priority|wrr|htb]`  
`no policy <policy-name>`

| Parameter     | Description                      |
|---------------|----------------------------------|
| <policy_name> | The name of the policy           |
| priority      | Use Priority Queueing (PQ)       |
| wrr           | Use Weighted Round Robin (WRR)   |
| htb           | Use Hierarchy Token Bucket (HTB) |

**Default** No policies are configured

**Mode** Traffic-Control

**Usage** A policy specifies a top-level queueing discipline which determines the type of classes that can be configured under the policy. This command uses the Traffic-Control Policy mode.

**Examples** To configure a policy, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#
```

To delete an existing policy, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#no policy p01 htb
```

**Related commands**

- [class \(htb\)](#)
- [class \(priority\)](#)
- [class \(wrr\)](#)
- [rule \(traffic-control\)](#)
- [traffic-control](#)
- [sub-class \(htb\)](#)

sub-class (priority)

sub-class (wrr)

sub-sub-class (htb)

sub-sub-class (priority)

sub-sub-class (wrr)

# red-curve

**Overview** Use this command to allow configuration of a RED (Random Early Discard) curve template.

Use the **no** variant of this command to set the RED curve back to the default.

**Syntax** `red-curve <red-curve-name> [limit <4-127>] [avpkt <64-1518>]  
[min <3-126>] [max <4-127>] [probability <1-100>]  
[ecn [ecn-drop]]  
no red-curve [<red-curve-name>]`

| Parameter           | Description                                                                                                                                                                     |
|---------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <red-curve-name>    | The RED curve name.                                                                                                                                                             |
| limit <4-127>       | The hard queue length limit (in packets) for the RED curve. Once the queue length reaches the limit, all packets are dropped.                                                   |
| avpkt <64-1518>     | The average packet size to use for queue size calculations in bytes.                                                                                                            |
| min <3-126>         | The minimum queue length for random early discard (in packets). Between <min> and <max> the drop probability will increase linearly.                                            |
| max <4-127>         | The maximum queue length where packets are probabilistically dropped. At <max> the drop probability equals <probability>. Beyond <max> the drop or marking probability is 100%. |
| probability <1-100> | The probability of a packet being dropped when queue-length reaches <max>. The drop probability increases linearly from 0 to <probability> in between <min> and <max>.          |
| ecn                 | Use explicit congestion notification marking instead of dropping the packet.                                                                                                    |
| ecn-drop            | When average queue size exceeds <max> drop packets instead of marking.                                                                                                          |

**Default** The default RED curve is **red-curve default limit 127 avpkt 576B min 10 max 32 prob 2**.

**Mode** Traffic-control

**Usage notes** The RED curve template can later be applied to a traffic control class, sub-class, or sub-sub-class.

**Example** To configure a RED curve with ECN dropping and the default curve shape, use the commands:

```
awplus# configure terminal
awplus(config)# traffic-control
awplus(config-tc)# red-curve red-ecn ecn
```

To configure an aggressive RED curve, use the commands:

```
awplus# configure terminal
awplus(config)# traffic-control
awplus(config-tc)# red-curve aggressive min 5 max 50
probability 70
```

**Related  
commands**

- class (htb)
- class (priority)
- class (wrr)
- show traffic-control policy
- show running-config traffic-control
- show traffic-control red-curve
- sub-class (htb)
- sub-class (priority)
- sub-class (wrr)
- sub-sub-class (htb)
- sub-sub-class (priority)
- sub-sub-class (wrr)



# rule (traffic-control)

**Overview** Use this command to create a traffic-control rule.

Use the **no** variant of this command to remove a traffic-control rule

**Syntax** `rule [<1-65535>] match <application> from <source-entity> to  
<destination-entity> policy <policy>  
no rule [<1-65535>]`

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-65535>            | The rule ID is an integer in the range from 1 to 65535. If you do not designate a rule ID, one will be automatically generated and it will be greater than the current highest rule ID. Lower IDs have higher priority.                                                                                                                                                          |
| match                | Application traffic to match                                                                                                                                                                                                                                                                                                                                                     |
| <application>        | Application name.<br>You can use the tab key to auto-complete application names.                                                                                                                                                                                                                                                                                                 |
| from                 | Set the source of the entity                                                                                                                                                                                                                                                                                                                                                     |
| <source_entity>      | Source entity name. Entities represent logical grouping of subnets, hosts or interfaces.<br>You can use the tab key to auto-complete entity names.                                                                                                                                                                                                                               |
| to                   | Set the destination of the entity                                                                                                                                                                                                                                                                                                                                                |
| <destination_entity> | Source entity name. Entities represent logical grouping of subnets, hosts or interfaces.                                                                                                                                                                                                                                                                                         |
| policy               | Policy to apply to matched traffic                                                                                                                                                                                                                                                                                                                                               |
| <policy>             | Traffic control policy. This consists of a top-level policy name followed by the name of a class within that policy, and sub-class (of the class) and a sub-sub-class if applicable. Examples are:<br>p01.c03<br>p01.c03.sc02<br>p01.c03.scc02.ssc01<br>In these examples, p01 is the policy name, c03 is the class name, sc02 is the sub-class, and ssc01 is the sub-sub-class. |

**Default** No rules

**Mode** Traffic-Control

**Usage** Rules are used to apply traffic-control policies to a type of traffic. When traffic control is enabled and no rules are added, a default traffic-control policy is installed on all supported interfaces.

If the application, source entity or destination entity specified in the rule is not configured correctly, the rule is not valid and is not installed.

You can change the rule order by using the move rule (traffic-control) command.

Rules are applied to destination interfaces in the order of their ID (lower IDs are applied first). If traffic matches a rule, then the rest are ignored. If traffic does not match any rule, then it is classified to the default class.

A rule can specify the system class as the policy. System traffic is high priority traffic that is allocated a fixed amount of bandwidth on an interface. Use the `interface (traffic-control)` command to configure system bandwidth on an interface.

**Examples** To configure a rule, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#rule 10 match ftp from wan to private policy
p01.c02.sc03
```

To delete a rule, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#no rule 10
```

**Related  
commands**

[interface \(traffic-control\)](#)  
[move rule \(traffic-control\)](#)  
[policy \(traffic-control\)](#)  
[traffic-control](#)  
[show running-config traffic-control](#)  
[show traffic-control rule](#)

# show debugging traffic-control

**Overview** Use this command to display the status of traffic control debugging

**Syntax** `show debugging traffic-control`

**Mode** Privileged Exec

**Example** To show if traffic-control debugging is on or off, run the command:

```
awplus#show debugging traffic-control
```

**Output** Figure 33-1: Example output from **show debugging traffic-control**

```
awplus#show debugging traffic-control
Traffic-control Debugging Status: off
```

**Related commands** [debug traffic-control](#)  
[show debugging](#)

# show running-config traffic-control

**Overview** Use this command to display the current traffic control configuration.

Note that Vista Manager EX will dynamically set the virtual bandwidth if you use its Auto Traffic Shaping feature. In that situation, this command will display the [interface dynamic-virtual-bandwidth](#) command instead of any virtual bandwidth added with the [interface \(traffic-control\)](#) command.

**Syntax** `show running-config traffic-control`

**Mode** Privileged Exec

**Example** To show the traffic control configuration section of the running configuration, use the command:

```
awplus#show running-config traffic-control
```

**Output** Figure 33-2: Example output from **show running-config traffic-control**

```
awplus#show running-config traffic-control
traffic-control
policy p1 priority
class c1 priority-level 15
rule 10 match selfmade1 from lan to inet policy p1.c1
traffic-control enable
!
```

**Related commands**

- [interface \(traffic-control\)](#)
- [show running-config](#)
- [show traffic-control counters](#)
- [show traffic-control interface](#)
- [show traffic-control policy](#)
- [show traffic-control rule](#)
- [show traffic-control rule config-check](#)
- [traffic-control](#)

**Command changes** Version 5.5.0-1.1: behavior changed when Auto Traffic Shaping is enabled in Vista Manager EX

# show traffic-control counters

**Overview** Use this command to display counters related to traffic control. This command displays counters for the number of packets sent, queued or dropped by each traffic control class. The information is shown by each interface. There is an overall counter for the policy, and counters for each leaf class in the policy.

If no interface name is specified then information for all interfaces with traffic control policies applied is displayed.

**Syntax** `show traffic-control counters [<interface-name>]`

| Parameter                           | Description                                           |
|-------------------------------------|-------------------------------------------------------|
| <code>&lt;interface-name&gt;</code> | Name of Interface to display traffic control counters |

**Mode** Privileged Exec

**Examples** To show the traffic control counters for all interfaces, use the commands:

```
awplus#show traffic-control counters
```

Figure 33-3: Example output from **show traffic-control counters**

|                                      |                  |       |         |
|--------------------------------------|------------------|-------|---------|
| awplus#show traffic-control counters |                  |       |         |
| Traffic Control Counters             |                  |       |         |
| Interface eth1:                      |                  |       |         |
| Class                                | Counter          | Bytes | Packets |
| -----                                |                  |       |         |
| A                                    | Sent             | 0     | 0       |
|                                      | Currently Queued | 0     | 0       |
|                                      | Dropped          |       | 0       |
| A.B5001                              | Sent             | 0     | 0       |
|                                      | Currently Queued | 0     | 0       |
|                                      | Dropped          |       | 0       |
| A.B5002                              | Sent             | 0     | 0       |
|                                      | Currently Queued | 0     | 0       |
|                                      | Dropped          |       | 0       |
| A.default                            | Sent             | 0     | 0       |
|                                      | Currently Queued | 0     | 0       |
|                                      | Dropped          |       | 0       |
| system                               | Sent             | 0     | 0       |
|                                      | Currently Queued | 0     | 0       |
|                                      | Dropped          |       | 0       |

| Interface eth2: |                  |          |         |
|-----------------|------------------|----------|---------|
| Class           | Counter          | Bytes    | Packets |
| -----           |                  |          |         |
| A               | Sent             | 58681224 | 232862  |
|                 | Currently Queued | 0        | 383     |
|                 | Dropped          |          | 1039845 |
| A.B5001         | Sent             | 10671444 | 42347   |
|                 | Currently Queued | 32004    | 128     |
|                 | Dropped          |          | 164954  |
| A.B5002         | Sent             | 17661924 | 70087   |
|                 | Currently Queued | 32004    | 127     |
|                 | Dropped          |          | 123470  |
| A.default       | Sent             | 30348360 | 120430  |
|                 | Currently Queued | 32004    | 128     |
|                 | Dropped          |          | 751421  |
| system          | Sent             | 42       | 1       |
|                 | Currently Queued | 0        | 0       |
|                 | Dropped          |          | 0       |

**Related commands** [show running-config traffic-control](#)

# show traffic-control interface

**Overview** Use this command to display information about interfaces known to traffic control, such as the applied policy, the virtual-bandwidth configured on the interface, the bandwidth reserved for system traffic and the overhead applied to the packet size calculations. If no interface name is specified, information is shown for all interfaces known to traffic control.

**Syntax** `show traffic-control interface [<interface-name>]`

| Parameter        | Description                              |
|------------------|------------------------------------------|
| <interface-name> | Name of interface to display information |

**Mode** Privileged Exec

**Examples** To show traffic control information for all interfaces, use the command:

```
awplus#show traffic-control interface
```

**Output** Figure 33-4: Example output from **show traffic-control interface**

```
awplus#show traffic-control interface
Traffic Control Interface Information

eth1:

Policy: A
Virtual bandwidth: Not set (optional)
System bandwidth: 5%
Packet overhead: 0 Bytes

eth2:

Policy: A
Virtual bandwidth: 2000 kbit
System bandwidth: 5%
Packet overhead 24 Bytes (Ethernet transport layer)

vlan1:

Policy: Default policy
Virtual bandwidth: Not set (optional)
Packet overhead: 0 Bytes

vlan10:

Policy: Default policy
Virtual bandwidth: Not set (optional)
Packet overhead: 0 Bytes
```

**Related commands** [interface \(traffic-control\)](#)  
[show running-config traffic-control](#)

# show traffic-control policy

**Overview** Use this command to show information about the configured traffic control policies and classes. This command shows the configured traffic control policies and the interfaces that they are applied to. Only non-default configuration parameters are shown.

If no policy name is given, all configured policies are displayed.

**Syntax** `show traffic-control policy [<policy-name>]`

| Parameter     | Description               |
|---------------|---------------------------|
| <policy-name> | Name of policy to display |

**Mode** Privileged Exec

**Examples** To show all traffic control policies, use the command:

```
awplus#show traffic-control policy
```

**Output** Figure 33-5: Example output from **show traffic-control policy**

```
awplus#show traffic-control policy
Traffic Control Policies:
Policy A:
 Type: wrd
 Applied interfaces: eth1 eth2
 Classes:
 Class B5001:
 Weight: 30
 Class B5002:
 Weight: 60
 Red curve: default
Policy P:
 Type: priority
 Applied interfaces: None
 Classes:
 Class P10:
 Priority: 10
 Peak rate (PIR): 5000kbit
 Class P3:
 Priority: 3
 Peak rate (PIR): 8000kbit
 Sub-queue type: htb
 Red curve TCP_session_1
```



```
Class H:
 Committed rate (CIR): 3000kbit
 Burst (Bc): 100000B
Class I:
 Committed rate (CIR): 5000kbit
 Burst (Bc): 100000B
Class P2:
 Priority: 2
 Red curve: TCP_session_2
Policy token-bucket:
 Type: htb
 Applied interfaces: None
Classes:
 Class A:
 Committed rate (CIR): 5000kbit
 Peak rate (PIR): 6000kbit
 Preference: 2
 Class B:
 Committed rate (CIR): 2000kbit
 Peak rate (PIR): 4000kbit
 Burst (Bc): 100000B
 Excess Burst (Be): 100000B
 Preference: 3
 Sub-queue type: htb
 Class C:
 Committed rate (CIR): 2000kbit
 Peak rate (PIR): 4000kbit
 Burst (BC): 50000B
 Class D:
 Committed rate (CIR): 1000kbit
 Peak rate (PIR): 4000kbit
 Burst (Bc): 50000B
 Sub-queue type: htb
 Class E:
 Committed rate (CIR): 500kbit
 Peak rate (PIR): 4000kbit
 Burst (Bc): 50000B
 Set DSCP: af23
 Class F:
 Committed rate (CIR): 500kbit
 Peak rate (PIR): 4000kbit
 Burst (Bc): 50000B
 Set DSCP: af31
```

**Related commands** [show running-config](#)  
[show running-config traffic-control](#)

# show traffic-control red-curve

**Overview** Use this command to show configured RED curve templates.

**Syntax** `show traffic-control red-curve <red-curve-name>`

| Parameter                           | Description                                                                                                             |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;red-curve-name&gt;</code> | The name of the RED curve. The default RED curve is <b>red-curve default limit 127 avpkt 576B min 10 max 32 prob 2.</b> |

**Mode** Privileged Exec

**Usage notes** If you have not configured some parameters, default values will display. If no RED curve name is given, all configured RED curves are shown.

**Example** To show all RED curves, use the command:

```
awplus# show traffic-control red-curve
```

To show a specified red curve called "TCP\_session\_1", use the command:

```
awplus# show traffic-control red-curve TCP_session_1
```

**Output** Figure 33-6: Example output from **show traffic-control red-curve**

```
awplus#show traffic-control red-curve
Traffic Control RED Curves:

RED curve default:
 Average packet size: 576 bytes
 Minimum: 10 packets
 Maximum: 32 packets
 Limit: 127 packets
 Drop probability: 2%
 ECN marking: disabled

RED curve TCP_session_1:
 Average packet size: 576 bytes
 Minimum: 20 packets
 Maximum: 60 packets
 Limit: 127 packets
 Drop probability: 20%
 ECN marking: disabled
```

Figure 33-7: Example output from **show traffic-control red-curve TCP\_session\_1**

```
awplus#show traffic-control red-curve TCP_session_1
Traffic Control RED Curves
RED curve TCP_session_1:
Average packet size: 576 bytes
Minimum: 20 packets
Maximum: 60 packets
Limit: 127 packets
Drop probability: 20%
ECN marking: disabled
```

**Related commands**

- [red-curve](#)
- [show running-config](#)
- [show running-config traffic-control](#)
- [show traffic-control policy](#)

# show traffic-control rule config-check

**Overview** Use this command to show information about traffic control rule validity.

**Syntax** `show traffic-control rule config-check`

**Mode** Privileged Exec

**Usage** An asterisk is printed before each rule that is invalid. To help determine why the rule is invalid, the `show traffic-control rule config-check` command will print the reasons why the rule is invalid. Information is only shown for invalid rules. If all rules are valid, a message will be printed showing all rules are valid.

**Example** To check if configured rules are valid, use the commands:

```
awplus#show traffic-control rule config-check
```

**Output** Figure 33-8: Example output from **show traffic-control rule config-check**

```
awplus#show traffic-control rule config-check

Rule 30:
 "From" entity does not exist
 "To" entity does not exist
 Policy doesn't exist or is not leaf
```

**Related commands**

- [move rule \(traffic-control\)](#)
- [rule \(traffic-control\)](#)
- [show traffic-control rule](#)
- [show running-config traffic-control](#)

# show traffic-control rule

**Overview** Use this command to show specific rules or a complete list of rules configured for traffic control.

**Syntax** `show traffic-control rule [<1-65535>]`

| Parameter | Description                                                                           |
|-----------|---------------------------------------------------------------------------------------|
| <1-65535> | The ID of the rule you want to display. If no ID is entered, all rules are displayed. |

**Mode** Privileged Exec

**Usage** An asterisk will be printed at the start of a row if the rule is invalid. The rules are shown in a table showing the rule ID, the application, source and destination that the rule matches on and the policy and class that the matching traffic will be sent to.

**Examples** To show a list of all traffic control rules configured, use the command:

```
awplus#show traffic-control rule
```

To show traffic control rule 10 configured, use the command:

```
awplus#show traffic-control rule 10
```

**Output** Figure 33-9: Example output from **show traffic-control rule**

|                                                                        |          |            |           |           |
|------------------------------------------------------------------------|----------|------------|-----------|-----------|
| awplus#show traffic-control rule                                       |          |            |           |           |
| [* - Rule is not valid - see "show traffic-control rule config-check"] |          |            |           |           |
| ID                                                                     | APP      | From       | To        | Policy    |
| -----                                                                  |          |            |           |           |
| 10                                                                     | udp-5001 | ipv6.vlan3 | ipv6.eth2 | A.B5001   |
| 20                                                                     | udp-5002 | ipv6.vlan3 | ipv6.eth2 | A.B5002   |
| * 30                                                                   | aserf    | asdf       | fasdf     | sadf.asdf |

**Related commands**

- [move rule \(traffic-control\)](#)
- [rule \(traffic-control\)](#)
- [show running-config traffic-control](#)
- [show traffic-control](#)
- [show traffic-control rule config-check](#)

# show traffic-control

**Overview** Use this command to display a brief overview of the status of the traffic control information on the router.

**Syntax** `show traffic-control`

**Mode** Privileged Exec

**Usage** This command shows if traffic control is enabled, how many rules are configured and how many interfaces have a virtual bandwidth applied.

**Example** To show an overview of the status of the traffic control information, use the commands:

```
awplus# show traffic-control
```

**Output** Figure 33-10: Example output from **show traffic-control**

```
awplus#show traffic-control
Traffic control is enabled
Policy configured on 5 interfaces
2 rules configured (2 valid rules)
Virtual-bandwidth configured on 1 interfaces
```

**Related commands** [traffic-control](#)  
[traffic-control enable](#)

## sub-class (htb)

**Overview** Use this command to configure a hierarchy token bucket (HTB) sub-class within an existing class.

Use the **no** variant of this command to delete an existing sub-class under the current class.

**Syntax**

```
sub-class <class-name> [cir <committed-rate>] [pir <peak-rate>]
[bc <1-100000000>] [be <1-100000000>] [preference <0-7>]
[queue-length <2-65536>] [set-dscp <dscp-value>] [red-curve
<red-curve-name>]

sub-class <class-name> [cir <committed-rate>] [pir <peak-rate>]
[bc <1-100000000>] [be <1-100000000>] [preference <0-7>]
sub-sub-class-policy htb

no sub-class <class-name>
```

| Parameter                  | Description                                                                                                                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <class-name>               | Name of the class.                                                                                                                                                                                                                            |
| cir <committed-rate>       | Set the Committed Information Rate (CIR) for the queue. Specified in kbit/mbit/gbit per second, 1kbit-100gbit.<br>This parameter is compulsory when creating a new sub-class. When editing an existing sub-class, this parameter is optional. |
| pir <peak-rate>            | Set the Peak Information Rate (PIR) for the queue. This is the rate of the queue under peak conditions. Specified in kbit/mbit/gbit per second, in the range 1kbit-100gbit.                                                                   |
| bc <1-100000000>           | Set the Committed Burst size (BC). This is the burst allowed above the CIR, sent at the PIR rate.                                                                                                                                             |
| be <1-100000000>           | Set the Excess Burst size (BE). This is the burst allowed above the PIR, sent at the maximum rate.                                                                                                                                            |
| preference <0-7>           | Set the preference for a class to receive spare bandwidth (highest is 7).                                                                                                                                                                     |
| queue-length <2-65536>     | Set the maximum queue length in packets.                                                                                                                                                                                                      |
| set-dscp <dscp-value>      | Set the DSCP value to apply to the packets.                                                                                                                                                                                                   |
| red-curve <red-curve-name> | Apply a random early discard template with the sub-class and enter the name of the red curve template to apply.                                                                                                                               |
| sub-sub-class-policy       | Specify that the sub-class will contain sub-sub-classes.                                                                                                                                                                                      |
| htb                        | Sub-sub-classes will use the Hierarchy Token Bucket (HTB) queueing discipline.                                                                                                                                                                |

**Default** BC and BE are assigned suitable values proportional to the CIR and PIR respectively and are larger than the MTU. PIR defaults to the CIR. Preference defaults to 7 and the queue length default to 1000 if the class is a leaf.

**Mode** Traffic-Control Class for an HTB sub-class policy.

**Usage** If there is already a sub-class in the same level with the specified name, the command will replace the configuration of the existing sub class if it does not have any sub-sub-classes.

If you specify a sub-sub-class policy, this command puts you into sub-class mode so you can specify the sub-sub-class.

**Examples** To configure a leaf sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01 cir 100mbit pir 150mbit
sub-class-policy htb
wplus(config-tc-class)#sub-class s02 cir 20mbit queue-length
200 red-curve s02-red
```

To enter Traffic-Control Class mode for an existing sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#
```

To delete an existing sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#no sub-class s01
```

**Related commands**

- [class \(htb\)](#)
- [class \(priority\)](#)
- [policy \(traffic-control\)](#)
- [sub-sub-class \(htb\)](#)
- [traffic-control](#)



## sub-class (priority)

**Overview** Use this command to configure a priority queue sub-class within a class.

Use the **no** variant of this command to delete an existing sub-class under the current class.

**Syntax**

```
sub-class <class-name> [priority-level <0-15>] [max <max-rate>]
[queue-length <2-65536>] [set-dscp <dscp_value>] [red-curve
<red-curve-name>]

sub-class <class-name> [priority-level <0-15>]
sub-sub-class-policy {priority|wrr|htb}

no sub-class <class-name>
```

| Parameter                  | Description                                                                                                                                                                |
|----------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <class-name>               | Name of the class.                                                                                                                                                         |
| priority-level <0-15>      | Set the priority level (15 is the highest).<br>This parameter is compulsory when creating a new sub-class. When editing an existing sub-class, this parameter is optional. |
| max <max-rate>             | Set the maximum traffic rate of the queue (in kbit/mbit/gbit per second, 1kbit-100gbit).                                                                                   |
| queue-length <2-65536>     | Set the maximum queue length in packets.                                                                                                                                   |
| set-dscp<dscp-value>       | Set the DSCP value to apply to the packets.                                                                                                                                |
| red-curve <red-curve-name> | Apply a random early discard template with the sub class and enter the name of the red curve template to apply.                                                            |
| sub-sub-class-policy       | Create a sub-sub-class for the policy.                                                                                                                                     |
| priority                   | Sub-sub-classes will use the Priority Queue queueing algorithm.                                                                                                            |
| wrr                        | Sub-sub-classes will use the Weighted Round Robin (WRR) queueing algorithm.                                                                                                |
| htb                        | Sub-classes will use the Hierarchy Token Bucket (HTB) queueing algorithm.                                                                                                  |

**Default** A priority queue sub class has no max rate, DSCP value or sub-sub class policy. The queue length is 1000 by default if the class is a leaf.

**Mode** Traffic-Control Class for a priority sub-class policy.

**Usage** If there is already a sub-class in the same level with the specified name, the command will replace the configuration of the existing sub class if it does not have any sub-sub classes.

If a sub-sub class policy is specified, this command uses the Traffic-Control Class mode to apply it.

**Examples** To configure a sub-class as the leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01 priority-level 5
sub-class-policy priority
awplus(config-tc-class)#sub-class s02 priority-level 8 max
50mbit queue-length 200 red-curve ss01-red
```

To enter Traffic-Control Class mode for an existing sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#
```

To delete an existing class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#no sub-class s01
```

**Related  
commands**

[class \(priority\)](#)  
[policy \(traffic-control\)](#)  
[sub-sub-class \(htb\)](#)  
[sub-sub-class \(priority\)](#)  
[sub-sub-class \(wrr\)](#)  
[traffic-control](#)

## sub-class (wrr)

**Overview** Use this command to configure a Weighted Round-Robin (WRR) sub-class within a class.

Use the **no** variant of this command to delete an existing sub-class under the current class.

**Syntax**

```
sub-class <class-name> [weight <1-100>] [queue-length
<2-65536>] [set-dscp <dscp-value>] [red-curve
<red-curve-name>]

sub-class <class-name> [weight <1-100>] sub-sub-class-policy
wrr

no sub-class <class-name>
```

| Parameter                  | Description                                                                                                                                                                                                                                                                           |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <class-name>               | Name of the sub-class.                                                                                                                                                                                                                                                                |
| weight<1-100>              | Set the weight. The relative weight is the available bandwidth divided between sibling WRR classes according to the ratio of their configured weights.<br>This parameter is compulsory when creating a new sub-class. When editing an existing sub-class, this parameter is optional. |
| queue-length<2-65536>      | Set the maximum queue length in packets.                                                                                                                                                                                                                                              |
| set-dscp                   | Set the DSCP value to apply to packets.                                                                                                                                                                                                                                               |
| <dscp-value>               | DSCP value as an integer or lower-case DSCP name.                                                                                                                                                                                                                                     |
| red curve <red-curve-name> | Apply a random early discard template with the sub-class and enter the name of the red curve template to apply.                                                                                                                                                                       |
| sub-sub-class-policy       | Create a sub-sub-class within the policy.                                                                                                                                                                                                                                             |
| wrr                        | Sub sub classes use the Weighted Round Robin queueing discipline.                                                                                                                                                                                                                     |

**Default** A weighted round-robin sub class has no DSCP value or sub-sub-class policy. The queue length is 1000 by default.

**Mode** Traffic-Control Class for a WRR sub-class policy.

**Usage** If there is already a class in the same level with the specified name, the command will replace the configuration of the existing class if it does not have any sub-classes.

If a sub class policy is specified, this command uses the Traffic-Control Class mode to apply it.

**Examples** To configure a sub-class as a leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 wrr
awplus(config-tc-policy)#class c02 weight 30 sub-class-policy
wrr
awplus(config-tc-class)#sub-class s02 weight 40 queue-length
200 red-curve s02-red
```

To enter Traffic-Control Class mode for an existing sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#
```

To delete an existing sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#no sub-class s01
```

**Related  
commands**

[class \(priority\)](#)  
[class \(wrr\)](#)  
[policy \(traffic-control\)](#)  
[traffic-control](#)  
[sub-sub-class \(wrr\)](#)

## sub-sub-class (htb)

**Overview** Use this command to configure a Hierarchy Token Bucket (HTB) sub-sub-class for a sub-class.

Use the **no** variant of this command to delete an existing sub-sub-class from the current sub-class.

**Syntax** `sub-sub-class <class-name> [cir <committed-rate>] [pir <peak-rate>] [bc <1-100000000>] [be <1-100000000>] [preference <0-7>] [queue-length <2-65536>] [set-dscp <dscp-value>] [red-curve <red-curve-name>]`  
`no sub-sub-class <class-name>`

| Parameter                                     | Description                                                                                                                                                                                                                                           |
|-----------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;class-name&gt;</code>               | Name of the sub-sub-class.                                                                                                                                                                                                                            |
| <code>cir &lt;committed-rate&gt;</code>       | Set the Committed Information Rate (CIR) for the queue. Specified in kbit/mbit/gbit per second, 1kbit-100gbit.<br>This parameter is compulsory when creating a new sub-sub-class. When editing an existing sub-sub-class, this parameter is optional. |
| <code>pir &lt;peak-rate&gt;</code>            | Set the Peak Information Rate (PIR) for the queue. This is the rate of the queue under peak conditions. Specified in kbit/mbit/gbit per second, in the range 1kbit-100gbit.                                                                           |
| <code>bc &lt;1-100000000&gt;</code>           | Set the Committed Burst size (BC). This is the burst allowed above the CIR, sent at the PIR rate.                                                                                                                                                     |
| <code>be &lt;1-100000000&gt;</code>           | Set the Excess Burst size (BE. This is the burst allowed above the PIR, sent at the maximum rate..                                                                                                                                                    |
| <code>preference &lt;0-7&gt;</code>           | Set the preference for a class to receive spare bandwidth (highest is 7).                                                                                                                                                                             |
| <code>queue-length &lt;2-65536&gt;</code>     | Set the maximum queue length.                                                                                                                                                                                                                         |
| <code>set-dscp &lt;dscp-value&gt;</code>      | Set the DSCP value to apply to the packets.                                                                                                                                                                                                           |
| <code>red-curve &lt;red-curve-name&gt;</code> | Apply a random early discard template with the sub-sub-class and enter the name of the red curve template to apply.                                                                                                                                   |

**Default** BC and BE are assigned suitable values proportional to the CIR and PIR respectively and are larger than the MTU. PIR defaults to the CIR. Preference defaults to 7 and Queue length defaults to 1000.

**Mode** Traffic-Control Sub-class for an HTB sub-sub-class policy.

**Usage** If there is already a sub-sub-class in the same level with the specified name, this command will replace the configuration of the existing sub-sub-class.

**Examples** To configure a sub-sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01 cir 100mbit pir 150mbit
sub-class-policy htb
awplus(config-tc-class)#sub-class s01 cir 10mbit
```

To configure a leaf sub-sub-class with a RED curve, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01 cir 100mbit pir 150mbit
sub-class-policy htb
awplus(config-tc-class)#sub-class s01 cir 10mbit
sub-sub-class-policy htb
awplus(config-tc-subclass)#sub-sub-class ss01 cir 5mbit
queue-length 200 red-curve ss01-red
```

To delete an existing sub-sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#no sub-sub-class ss01
```

**Related commands**

- [policy \(traffic-control\)](#)
- [sub-class \(htb\)](#)
- [sub-class \(priority\)](#)
- [traffic-control](#)

## sub-sub-class (priority)

**Overview** Use this command to configure a priority queue sub-sub-class for a sub-class.

Use the **no** variant of this command to delete an existing sub-sub-class from the current sub-class.

**Syntax** `sub-sub-class <class-name> [priority-level <0-15>] [max <max-rate>] [queue-length <2-65536>] [set-dscp <dscp-value>] [red-curve <red-curve-name>]`

`no sub-sub-class <class-name>`

| Parameter                  | Description                                                                                                                                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <class-name>               | Name of the class.                                                                                                                                                              |
| priority-level <0-15>      | Set the priority level (15 is the highest). This parameter is compulsory when creating a new sub-sub-class. When editing an existing sub-sub-class, this parameter is optional. |
| max <max-rate>             | Set the maximum traffic rate of the queue (in kbit/mbit/gbit per second, 1kbit-100gbit).                                                                                        |
| queue-length <2-65536>     | Set the maximum queue length in packets.                                                                                                                                        |
| set-dscp <dscp-value>      | Set the DSCP value to apply to the packets.                                                                                                                                     |
| red-curve <red-curve-name> | Apply a random early discard template with the sub-sub-class and enter the name of the red curve template to apply.                                                             |

**Default** A priority queue sub-sub-class has no max rate or DSCP value. The queue length is 1000.

**Mode** Traffic-Control Sub-class for a priority sub-sub-class policy.

**Usage** If there is already a sub-sub-class in the same level with the specified name, this command will replace the configuration of the existing sub-sub-class.

**Examples** To configure a sub-sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01 priority-level 5
awplus(config-tc-class)#sub-class s01 priority-level 7
awplus(config-tc-subclass)#sub-sub-class ss01 priority-level 3
```

To configure a sub-sub-class with a RED curve, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 priority
awplus(config-tc-policy)#class c01 priority-level 5
sub-class-policy priority
awplus(config-tc-class)#sub-class s01 priority-level 7
sub-sub-class-policy priority
awplus(config-tc-subclass)#sub-sub-class ss01 priority-level 3
max 5mbit queue-length 200 red-curve ss01-red
```

To delete an existing sub-sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#no sub-sub-class ss01
```

**Related commands**

- [traffic-control](#)
- [policy \(traffic-control\)](#)
- [sub-class \(priority\)](#)



## sub-sub-class (wrr)

**Overview** Use this command to configure a Weighted Round-Robin (WRR) sub-sub-class within a sub-class.

Use the **no** variant of this command to delete an existing sub-sub-class from the current sub-class.

**Syntax** `sub-sub-class <class-name> [weight <1-100>] [queue-length <2-65536>] [set-dscp <dscp-value>] [red-curve <red-curve-name>]`  
`no sub-sub-class <class-name>`

| Parameter                                     | Description                                                                                                                                                                                                                                                                                   |
|-----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;class-name&gt;</code>               | Name of the sub-class.                                                                                                                                                                                                                                                                        |
| <code>weight &lt;1-100&gt;</code>             | Set the weight. The relative weight is the available bandwidth divided between sibling WRR classes according to the ratio of their configured weights.<br>This parameter is compulsory when creating a new sub-sub-class. When editing an existing sub-sub-class, this parameter is optional. |
| <code>queue-length &lt;2-65536&gt;</code>     | Set the maximum queue length in packets.                                                                                                                                                                                                                                                      |
| <code>set-dscp &lt;dscp-value&gt;</code>      | Set the DSCP value to apply to packets.                                                                                                                                                                                                                                                       |
| <code>red-curve &lt;red-curve-name&gt;</code> | Apply a random early discard template with the sub-sub-class and enter the name of the red curve template to apply.                                                                                                                                                                           |

**Default** A weighted round-robin sub-sub-class has no DSCP value. The queue length is 1000 by default.

**Mode** Traffic-Control Sub-class for a WRR sub-sub-class policy.

**Usage** If there is already a sub-sub-class in the same level with the specified name, this command will replace the configuration of the existing sub-sub-class.

**Examples** To configure a sub-sub-class as a leaf class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 wrr
awplus(config-tc-policy)#class c01 weight 50 sub-class-policy
wrr
awplus(config-tc-class)#sub-class s01 weight 30 sub-sub-class
policy wrr
awplus(config-tc-subclass)#sub-sub-class ss01 weight 5
queue-length 200
```

To configure a sub-sub-class with a RED curve, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 wrr
awplus(config-tc-policy)#class c01 weight 50 sub-class-policy
wrr
awplus(config-tc-class)#sub-class s01 weight 30
sub-sub-class-policy wrr
awplus(config-tc-subclass)#sub-sub-class ss01 weight 5
queue-length 200 red-curve ss01-red
```

To delete an existing sub-sub-class, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#policy p01 htb
awplus(config-tc-policy)#class c01
awplus(config-tc-class)#sub-class s01
awplus(config-tc-subclass)#no sub-sub-class ss01
```

**Related  
commands**

[traffic-control](#)  
[policy \(traffic-control\)](#)  
[sub-class \(priority\)](#)  
[sub-class \(wrr\)](#)

# traffic-control enable

- Overview** Use this command to enable traffic control.
- Use the **no** variant of this command to disable traffic control without losing your existing traffic control configuration.
- Syntax** `traffic-control enable`  
`no traffic-control enable`
- Default** Disabled
- Mode** Traffic-Control
- Usage** When traffic control is enabled and no rules are added, a default queueing discipline is applied to all interfaces that support traffic control. You can use the `policy` command to configure traffic control policies and the `rule (traffic-control)` command to apply the configured policies to the traffic.
- Examples** To enable traffic control, use the commands:
- ```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#traffic-control enable
```
- To disable traffic control, use the commands:
- ```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#no traffic-control enable
```
- Related commands** [policy \(traffic-control\)](#)  
[rule \(traffic-control\)](#)  
[traffic-control](#)

# traffic-control

**Overview** Use this command to enter into Traffic-Control configuration mode.  
Use the **no** variant of this command to remove all traffic control configuration.

**Syntax** `traffic-control`  
`no traffic-control`

**Default** Disabled

**Mode** Global Configuration

**Usage** This command enters you into Traffic-Control configuration mode.  
In Traffic-Control Configuration mode you can:

- enable or disable traffic control
- create and delete traffic control policies
- create, move and delete rules for traffic control
- set and unset packet overhead, system bandwidth and virtual bandwidth of interfaces

**Examples** To configure traffic-control, use the commands:

```
awplus#configure terminal
awplus(config)#traffic-control
awplus(config-tc)#
```

To remove all traffic control configuration, use the commands:

```
awplus#configure terminal
awplus(config)#no traffic-control
awplus(config)#
```

**Related commands**

- [class \(htb\)](#)
- [class \(priority\)](#)
- [class \(wrr\)](#)
- [debug traffic-control](#)
- [interface \(traffic-control\)](#)
- [move rule \(traffic-control\)](#)
- [policy \(traffic-control\)](#)
- [rule \(traffic-control\)](#)
- [traffic-control enable](#)
- [show debugging traffic-control](#)

show running-config traffic-control  
show traffic-control  
show traffic-control counters  
show traffic-control interface  
show traffic-control policy  
show traffic-control rule  
show traffic-control rule config-check  
sub-class (htb)  
sub-class (priority)  
sub-class (wrr)  
sub-sub-class (htb)  
sub-sub-class (priority)  
sub-sub-class (wrr)

# 34

# AAA Commands

## Introduction

**Overview** AAA is the collective title for the three related functions of Authentication, Authorization and Accounting. These functions can be applied in a variety of methods with a variety of servers.

The purpose of the AAA commands is to map instances of the AAA functions to sets of servers. The Authentication function can be performed in multiple contexts, such as authentication of users logging in at a console, or 802.1X-Authentication of devices connecting to Ethernet ports.

For each of these contexts, you may want to use different sets of servers for examining the proffered authentication credentials and deciding if they are valid. AAA Authentication commands enable you to specify which servers will be used for different types of authentication.

This chapter provides an alphabetical reference for AAA commands for Authentication, Authorization and Accounting. For more information, see the [AAA and Port\\_Authentication Feature Overview and Configuration Guide](#).

- Command List**
- [“aaa accounting commands”](#) on page 1580
  - [“aaa accounting login”](#) on page 1582
  - [“aaa accounting openvpn”](#) on page 1585
  - [“aaa accounting update”](#) on page 1587
  - [“aaa authentication 2fa-registration default group”](#) on page 1589
  - [“aaa authentication download-portal”](#) on page 1591
  - [“aaa authentication enable default group tacacs+”](#) on page 1593
  - [“aaa authentication enable default local”](#) on page 1595
  - [“aaa authentication isakmp”](#) on page 1596
  - [“aaa authentication login”](#) on page 1597
  - [“aaa authentication openvpn”](#) on page 1600

- [“aaa authorization commands”](#) on page 1602
- [“aaa authorization config-commands”](#) on page 1604
- [“aaa group server”](#) on page 1605
- [“aaa local authentication attempts logout-time”](#) on page 1607
- [“aaa local authentication attempts max-fail”](#) on page 1608
- [“aaa local authentication attempts max-fail remote-login-only”](#) on page 1609
- [“aaa login fail-delay”](#) on page 1610
- [“accounting login”](#) on page 1611
- [“authorization commands”](#) on page 1612
- [“clear aaa local user logout”](#) on page 1614
- [“debug aaa”](#) on page 1615
- [“login authentication”](#) on page 1616
- [“proxy-port”](#) on page 1617
- [“radius-secure-proxy aaa”](#) on page 1618
- [“server \(radsecproxy-aaa\)”](#) on page 1619
- [“server mutual-authentication”](#) on page 1621
- [“server name-check”](#) on page 1622
- [“server trustpoint”](#) on page 1623
- [“show aaa local user locked”](#) on page 1625
- [“show aaa server group”](#) on page 1627
- [“show debugging aaa”](#) on page 1628
- [“show radius server group”](#) on page 1629
- [“undebbug aaa”](#) on page 1631

# aaa accounting commands

**Overview** This command configures and enables TACACS+ accounting on commands entered at a specified privilege level. Once enabled for a privilege level, accounting messages for commands entered at that privilege level will be sent to a TACACS+ server.

In order to account for all commands entered on a device, configure command accounting for each privilege level separately.

The command accounting message includes, the command as entered, the date and time the command finished executing, and the user-name of the user who executed the command.

Use the **no** variant of this command to disable command accounting for a specified privilege level.

**Syntax** `aaa accounting commands <1-15> default stop-only group tacacs+`  
`no aaa accounting commands <1-15> default`

| Parameter | Description                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------|
| <1-15>    | The privilege level being configured, in the range 1 to 15.                                                        |
| default   | Use the default method list, this means the command is applied globally to all user exec sessions.                 |
| stop-only | Send accounting message when the commands have stopped executing.                                                  |
| group     | Specify the server group where accounting messages are sent. Only the tacacs+ group is available for this command. |
| tacacs+   | Use all TACACS+ servers configured by the <a href="#">tacacs-server host</a> command.                              |

**Default** TACACS+ command accounting is disabled by default.

**Mode** Global Configuration

**Usage notes** This command only supports a **default** method list, this means that it is applied to every console and VTY line.

The **stop-only** parameter indicates that the command accounting messages are sent to the TACACS+ server when the commands have stopped executing.

The **group tacacs+** parameters signifies that the command accounting messages are sent to the TACACS+ servers configured by the [tacacs-server host](#) command.

Note that up to four TACACS+ servers can be configured for accounting. The servers are checked for reachability in the order they are configured with only the first reachable server being used. If no server is found, the accounting message is dropped.



Command accounting cannot coexist with triggers. An error message is displayed if you attempt to enable command accounting while a trigger is configured. Likewise, an error message is displayed if you attempt to configure a trigger while command accounting is configured.

**Examples** To configure command accounting for privilege levels 1, 7, and 15, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting commands 1 default stop-only
group tacacs+
awplus(config)# aaa accounting commands 7 default stop-only
group tacacs+
awplus(config)# aaa accounting commands 15 default stop-only
group tacacs+
```

To disable command accounting for privilege levels 1, 7, and 15, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting commands 1 default
awplus(config)# no aaa accounting commands 7 default
awplus(config)# no aaa accounting commands 15 default
```

**Related commands**

- [aaa authentication login](#)
- [aaa accounting login](#)
- [accounting login](#)
- [tacacs-server host](#)

# aaa accounting login

**Overview** This command configures RADIUS and TACACS+ accounting for login shell sessions. The specified method list name can be used by the **accounting login** command in the Line Configuration mode. If the **default** parameter is specified, then this creates a default method list that is applied to every console and VTY line, unless another accounting method list is applied on that line.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to remove an accounting method list for login shell sessions configured by an **aaa accounting login** command. If the method list being deleted is already applied to a console or VTY line, accounting on that line will be disabled. If the default method list name is removed by this command, it will disable accounting on every line that has the default accounting configuration.

**Syntax**

```
aaa accounting login
{default|<list-name>} {start-stop|stop-only|none} {group
{radius|tacacs+|<group-name>}}

no aaa accounting login {default|<list-name>}
```

| Parameter    | Description                                                                                           |
|--------------|-------------------------------------------------------------------------------------------------------|
| default      | Default accounting method list.                                                                       |
| <list-name>  | Named accounting method list.                                                                         |
| start-stop   | Start and stop records to be sent.                                                                    |
| stop-only    | Stop records to be sent.                                                                              |
| none         | No accounting record to be sent.                                                                      |
| group        | Specify the servers or server group where accounting packets are sent.                                |
| radius       | Use all RADIUS servers configured by the <a href="#">radius-server host</a> command.                  |
| tacacs+      | Use all TACACS+ servers configured by the <a href="#">tacacs-server host</a> command.                 |
| <group-name> | Use the specified RADIUS server group, as configured by the <a href="#">aaa group server</a> command. |

**Default** Accounting for login shell sessions is disabled by default.

**Mode** Global Configuration

**Usage notes** This command enables you to define a named accounting method list. The items that you define in the accounting options are:

- the types of accounting packets that will be sent
- the set of servers to which the accounting packets will be sent

You can define a default method list with the name **default** and any number of other named method lists. The name of any method list that you define can then be used as the *<list-name>* parameter in the [accounting login](#) command.

If the method list name already exists, the command will replace the existing configuration with the new one.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by [radius-server host](#) command
- **group <group-name>** : use the specified RADIUS server group configured with the [aaa group server](#) command

There is one way to define servers where TACACS+ accounting messages are sent:

- **group tacacs+** : use all TACACS+ servers configured by [tacacs-server host](#) command

The accounting event to send to the RADIUS or TACACS+ server is configured with the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

**Examples** To configure RADIUS accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group
radius
```

To configure TACACS+ accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group
tacacs+
```

To reset the configuration of the default accounting list, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting login default
```

**Related  
commands**

- [aaa accounting commands](#)
- [aaa authentication login](#)
- [aaa accounting login](#)
- [accounting login](#)
- [radius-server host](#)
- [tacacs-server host](#)

# aaa accounting openvpn

**Overview** Use this command to configure the default accounting method list for OpenVPN tunnels. The default accounting method list specifies what type of accounting messages are sent and which RADIUS servers the accounting messages are sent to. The default accounting method list is automatically applied to OpenVPN tunnels.

Use the **no** variant of this command to disable AAA accounting for OpenVPN tunnels globally.

**Syntax** `aaa accounting openvpn default {start-stop|stop-only|none}  
group {<group-name>|radius}  
no aaa accounting openvpn default`

| Parameter    | Description                                                                                                               |
|--------------|---------------------------------------------------------------------------------------------------------------------------|
| default      | Configure the default accounting method list                                                                              |
| start-stop   | Sends a start accounting message at the beginning of the session and a stop accounting message at the end of the session. |
| stop-only    | Only sends a stop accounting message at the end of the session.                                                           |
| none         | No accounting record sent.                                                                                                |
| group        | Use a server group                                                                                                        |
| <group-name> | Server group name.                                                                                                        |
| radius       | Use all RADIUS servers.                                                                                                   |

**Default** RADIUS accounting for OpenVPN tunnels is disabled by default (there is no default server set by default).

**Mode** Global Configuration

**Usage notes** This command configures the default accounting method list which is automatically applied to all OpenVPN tunnels.

The accounting event to send to the RADIUS server is configured by the following options:

- **start-stop:** sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only:** sends a **stop** accounting message at the end of a session.
- **none:** disables accounting.

There are two ways to define servers where RADIUS accounting messages will be sent:

- **group radius:** use all RADIUS servers configured by [radius-server host](#) command.

- **group** <group-name>: use the specified RADIUS server group configured with the [aaa group server](#) command.

**Examples** To enable RADIUS accounting for OpenVPN tunnels, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting openvpn default start-stop group
radius
```

To disable RADIUS accounting for OpenVPN tunnels, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting openvpn default
```

**Related commands**

- [aaa accounting update](#)
- [aaa authentication openvpn](#)
- [aaa group server](#)
- [radius-server host](#)
- [show aaa server group](#)
- [tunnel mode openvpn tap](#)
- [tunnel mode openvpn tun](#)

**Command changes** Version 5.5.4-2.3: command added

# aaa accounting update

**Overview** This command enables periodic accounting reporting to either the RADIUS or TACACS+ accounting server(s) wherever login accounting has been configured.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to disable periodic accounting reporting to the accounting server(s).

**Syntax** `aaa accounting update [periodic <1-65535>]`  
`no aaa accounting update`

| Parameter                    | Description                                                                      |
|------------------------------|----------------------------------------------------------------------------------|
| <code>periodic</code>        | Send accounting records periodically.                                            |
| <code>&lt;1-65535&gt;</code> | The interval to send accounting updates (in minutes). The default is 30 minutes. |

**Default** Disabled

**Mode** Global Configuration

**Usage notes** Use this command to enable the device to send periodic AAA login accounting reports to the accounting server. When periodic accounting reporting is enabled, interim accounting records are sent at the interval specified by the **periodic** parameter. The accounting updates are start messages.

If the **no** variant of this command is used to disable periodic accounting reporting, any interval specified by the **periodic** parameter is reset to the default of 30 minutes when accounting reporting is re-enabled, unless this interval is specified.

**Examples** To configure the switch to send period accounting updates every 30 minutes, the default period, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update
```

To configure the switch to send period accounting updates every 10 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update periodic 10
```

To disable periodic accounting updates wherever accounting has been configured, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no aaa accounting update
```

**Related  
commands**

[aaa accounting login](#)

[radius-server host](#)



# aaa authentication 2fa-registration default group

**Overview** Use this command to set authentication methods for Two-Factor Authentication (2FA) user self-registration.

Use the **no** variant of this command to unset authentication methods for 2FA user self-registration.

**Syntax** `aaa authentication 2fa-registration default group {ldap|radius|<group-name>}`

`no aaa authentication 2fa-registration default`

| Parameter    | Description                                                                               |
|--------------|-------------------------------------------------------------------------------------------|
| ldap         | Use all LDAP servers configured by the <b>ldap-server name</b> command.                   |
| radius       | Use all RADIUS servers configured by the <b>radius-server host</b> command.               |
| <group-name> | The name of the LDAP or RADIUS server group to authenticate self-registration users with. |

**Default** No servers are configured by default

**Mode** Global Configuration

**Examples** To configure LDAP servers to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group ldap
```

To configure RADIUS servers to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group radius
```

To configure a selected LDAP or RADIUS group of servers called 'GRP1' to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group GRP1
```

To remove the configured server group for 2FA self-registration to authenticate with, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication 2fa-registration default
```

**Related commands**    [2fa self-registration port](#)  
[service 2fa](#)

**Command changes**    Version 5.5.3-0.1: command added

# aaa authentication download-portal

**Overview** Use this command to globally enable authentication, and set the default authentication method, for Download Portal clients. The default authentication method can be:

- all configured RADIUS servers,
- all configured LDAP servers,
- or a user-defined group of RADIUS or LDAP servers.

Use the **no** variant of this command to globally disable authentication on for Download Portal Clients.

**Syntax** `aaa authentication download-portal default group  
[<group-name>|radius|ldap]  
no aaa authentication download-portal default`

| Parameter    | Description            |
|--------------|------------------------|
| <group-name> | Server group name.     |
| radius       | Use all RADIUS servers |
| ldap         | Use all LDAP servers   |

**Default** Authentication for Download Portal clients is disabled by default.

**Mode** Global Configuration

**Usage notes** There are a number of ways to define groups of authentication servers. These are:

- **group radius:** use all RADIUS servers configured with the [radius-server host](#) command.
- **group ldap:** use all LDAP servers configured with the [ldap-server](#) command.
- **group <group-name>:** use the specified RADIUS or LDAP server group configured with the [aaa group server](#) command.

**Example** To enable LDAP authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication download-portal default
group ldap
```

To use a server group to authenticate Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication download-portal default
group my_group
```

**Note:** This could be a group of RADIUS or LDAP servers.

To disable authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication download-portal default
```

**Related  
commands**

[aaa group server](#)  
[download-portal](#)

**Command  
changes**

Version 5.5.4-0: command added

# aaa authentication enable default group tacacs+

**Overview** This command enables privilege level authentication against a TACACS+ server. Use the **no** variant of this command to disable privilege level authentication.

**Syntax** `aaa authentication enable default group tacacs+ [local] [none]`  
`no aaa authentication enable default`

| Parameter | Description                                                                                      |
|-----------|--------------------------------------------------------------------------------------------------|
| local     | Use the locally configured enable password ( <b>enable password</b> command) for authentication. |
| none      | No authentication.                                                                               |

**Default** Local privilege level authentication is enabled by default ([aaa authentication enable default local](#) command).

**Mode** Global Configuration

**Usage notes** A user is configured on a TACACS+ server with a maximum privilege level. When they enter the [enable \(Privileged Exec mode\)](#) command they are prompted for an enable password which is authenticated against the TACACS+ server. If the password is correct and the specified privilege level is equal to or less than the users maximum privilege level, then they are granted access to that level. If the user attempts to access a privilege level that is higher than their maximum configured privilege level, then the authentication session will fail and they will remain at their current privilege level.

**NOTE:** If both **local** and **none** are specified, you must always specify **local** first.

If the TACACS+ server goes offline, or is not reachable during enable password authentication, and command level authentication is configured as:

- **aaa authentication enable default group tacacs+**  
then the user is never granted access to Privileged Exec mode.
- **aaa authentication enable default group tacacs+ local**  
then the user is authenticated using the locally configured enable password, which if entered correctly grants the user access to Privileged Exec mode. If no enable password is locally configured (**enable password** command), then the enable authentication will fail until the TACACS+ server becomes available again.

- **aaa authentication enable default group tacacs+ none**

then the user is granted access to Privileged Exec mode with no authentication. This is true even if a locally configured enable password is configured.

- **aaa authentication enable default group tacacs+ local none**

then the user is authenticated using the locally configured enable password. If no enable password is locally configured, then the enable authentication will grant access to Privileged Exec mode with no authentication.

If the password for the user is not successfully authenticated by the server, then the user is again prompted for an enable password when they enter **enable** via the CLI.

**Examples** To enable a privilege level authentication method that will not allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authentication enable default group tacacs+
```

To enable a privilege level authentication method that will allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, and a locally configured enable password is configured, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authentication enable default group tacacs+
local
```

To disable privilege level authentication, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no aaa authentication enable default
```

**Related commands**

- [aaa authentication login](#)
- [aaa authentication enable default local](#)
- [enable \(Privileged Exec mode\)](#)
- [enable password](#)
- [enable secret \(deprecated\)](#)
- [tacacs-server host](#)

# aaa authentication enable default local

**Overview** This command enables local privilege level authentication.  
Use the **no** variant of this command to disable local privilege level authentication.

**Syntax** `aaa authentication enable default local`  
`no aaa authentication enable default`

**Default** Local privilege level authentication is enabled by default.

**Mode** Global Configuration

**Usage notes** The privilege level configured for a particular user in the local user database is the privilege threshold above which the user is prompted for an [enable \(Privileged Exec mode\)](#) command.

**Examples** To enable local privilege level authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default local
```

To disable local privilege level authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication enable default
```

**Related commands** [aaa authentication login](#)  
[enable \(Privileged Exec mode\)](#)  
[enable password](#)  
[enable secret \(deprecated\)](#)

# aaa authentication isakmp

**Overview** Use this command to enable global RADIUS authentication for ISAKMP tunnels. Use the **no** variant of this command to disable global RADIUS authentication of ISAKMP tunnels.

**Syntax** `aaa authentication isakmp default group [<group-name>|radius]`  
`no aaa authentication isakmp default`

| Parameter                       | Description            |
|---------------------------------|------------------------|
| <code>&lt;group-name&gt;</code> | Server group name      |
| <code>radius</code>             | Use all RADIUS servers |

**Default** Disabled

**Mode** Global Configuration

**Usage notes** When RADIUS authentication is enabled globally to ISAKMP tunnels it is automatically applied to every ISAKMP tunnel interface. There are two ways to define servers where radius accounting messages are sent:

- Group `radius`, where all RADIUS servers configured using this command are used
- Group `<group-name>`, where the specified RADIUS server group configured is used

**Examples** To enable RADIUS authentication for ISAKMP tunnels globally and use all available radius servers, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authentication isakmp default group radius
```

To disable RADIUS authentication for ISAKMP tunnels, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no authentication isakmp default
```

**Related commands** [radius-server host](#)  
[aaa group server](#)

**Command changes** Version 5.4.9-0.1: command added



# aaa authentication login

**Overview** Use this command to create an ordered list of methods for authenticating user logins. It can also be used to replace an existing method list with a list of the same name. Specify one or more of the options **local** or **group**, in the order you want them to be applied. If the **default** method list name is specified, it is applied to every console and VTY line immediately unless another method list is applied to that line by the [login authentication](#) command. To apply a non-default method list, you must also use the [login authentication](#) command.

Use the **no** variant of this command to remove a method list from user login authentication. The specified method list name is deleted from the configuration. If the method list name has been applied to any console or VTY line, user login authentication on that line will fail.

Note that the **no aaa authentication login default** command does not remove the default method list. This will return the default method list to its default state (**local** is the default).

**Syntax**

```
aaa authentication login {default|<list-name>} {[local] [group
{radius|ldap|tacacs+|<group-name>}]}
```

```
no aaa authentication login {default|<list-name>}
```

| Parameter    | Description                                                                           |
|--------------|---------------------------------------------------------------------------------------|
| default      | Set the default authentication server for user login.                                 |
| <list-name>  | Name of authentication server.                                                        |
| local        | Use the local username database.                                                      |
| group        | Use server group.                                                                     |
| radius       | Use all RADIUS servers configured by the <a href="#">radius-server host</a> command.  |
| ldap         | Use all LDAP servers configured by the <a href="#">ldap-server</a> command.           |
| tacacs+      | Use all TACACS+ servers configured by the <a href="#">tacacs-server host</a> command. |
| <group-name> | Use the specified RADIUS or LDAP server group.                                        |

**Default** If the default server is not configured using this command, user login authentication uses the local user database only.

If the **default** method list name is specified, it is applied to every console and VTY line immediately unless a named method list server is applied to that line by the **login authentication** command.

**local** is the default state for the default method list unless a named method list is applied to that line by the **login authentication** command. You can reset it to the default method list using the **no aaa authentication login default** command.

**Mode** Global Configuration

**Usage notes** When a user attempts to log in, the switch sends an authentication request to the first authentication server in the method list. If the first server in the list is reachable and it contains a username and password matching the authentication request, the user is authenticated and the login succeeds. If the authentication server denies the authentication request because of an incorrect username or password, the user login fails. If the first server in the method list is unreachable, the switch sends the request to the next server in the list, and so on.

For example, if the method list specifies **group tacacs+ local**, and a user attempts to log in with a password that does not match a user entry in the first TACACS+ server, if this TACACS+ server denies the authentication request, then the switch does not try any other TACACS+ servers nor the local user database; the user login fails.

**Examples** To configure the default authentication method list for user login to first use all available RADIUS servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login default group radius
local
```

To configure the default authentication method list for user login to first use all available LDAP servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login default group ldap
local
```

To configure a user login authentication method list called 'USERS' to first use the RADIUS server group 'RAD\_GROUP1' for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group RAD_GROUP1
local
```

To configure a user login authentication method list called 'USERS' to first use the TACACS+ servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group tacacs+
local
```

To return to the default method list (**local** is the default server), use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication login default
```

To delete an existing authentication method list 'USERS' created for user login authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication login USERS
```

**Related  
commands**

[aaa accounting commands](#)  
[aaa authentication enable default group tacacs+](#)  
[ldap-server](#)  
[login authentication](#)  
[radius-server host](#)

**Command  
changes**

Version 5.5.2-1.1: **ldap** parameter added

# aaa authentication openvpn

**Overview** Use this command to globally enable authentication, and set the default authentication method, on OpenVPN tunnels. The default authentication method can be:

- all configured RADIUS servers,
- all configured LDAP servers,
- or a user-defined group of RADIUS or LDAP servers.

In addition, you can optionally specify that two-factor authentication (2FA) is required on OpenVPN connections.

Use the **no** variant of this command to globally disable authentication on OpenVPN tunnels.

**Syntax**

```
aaa authentication openvpn default group
{<group-name>|radius|ldap} [2fa [2fa-in-password]]

no aaa authentication openvpn default
```

| Parameter       | Description                                        |
|-----------------|----------------------------------------------------|
| <group-name>    | Server group name.                                 |
| radius          | Use all RADIUS servers.                            |
| ldap            | Use all LDAP servers.                              |
| 2fa             | Require two-factor authentication (2FA).           |
| 2fa-in-password | Include the 2FA verification code in the password. |

**Default** Authentication on OpenVPN tunnels is disabled by default.

**Mode** Global Configuration

**Usage notes** There are a number of ways to define groups of authentication servers. These are:

- **group radius:** use all RADIUS servers configured with the [radius-server host](#) command.
- **group ldap:** use all LDAP servers configured with the [ldap-server](#) command.
- **group <group-name>:** use the specified RADIUS or LDAP server group configured with the [aaa group server](#) command.

The **2fa** parameter allows you to strengthen security by requiring a second method of authentication. It requires a software-based authenticator that implements the time-based one-time password (TOTP) or HMAC-based one-time password (HOTP) algorithms. These software authenticators (known as authenticator apps) are usually loaded on a mobile device. One well-known implementation of such an app is Google Authenticator.

The **2fa-in-password** parameter allows the user to enter their 2FA authentication code straight after their password in the password field of the OpenVPN client. For example, if their password is 'secret' and their OpenVPN code is '654321', they will enter 'secret654321' into the OpenVPN client's password field.

**Examples** To enable RADIUS authentication on OpenVPN tunnels and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication openvpn default group radius
```

To enable authentication on OpenVPN tunnels using the servers in group 'GROUP2', use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication openvpn default group GROUP2
```

Note: This could be a group of RADIUS or LDAP servers.

To enable LDAP authentication on OpenVPN tunnels, use all available LDAP servers, and require 2FA with the 2FA code in the password field, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication openvpn default group ldap
2fa 2fa-in-password
```

To disable authentication on OpenVPN tunnels, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication openvpn default
```

**Related commands** [aaa accounting openvpn](#)  
[aaa group server](#)  
[radius-server host](#)

**Command changes** Version 5.5.2-1.1: **ldap** and **2fa** parameters added

# aaa authorization commands

**Overview** This command configures a method list for commands authorization that can be applied to console or VTY lines. When command authorization is enabled for a privilege level, only authorized users can executed commands in that privilege level.

Use the **no** variant of this command to remove a named method list or disable the default method list for a privilege level.

**Syntax**

```
aaa authorization commands <privilege-level>
{default|<list-name>} group tacacs+ [none]

no aaa authorization commands <privilege-level>
{default|<list-name>}
```

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <privilege-level> | The privilege level of the set of commands the method list will be applied to.<br>AlliedWare Plus defines three sets of commands, that are indexed by a level value:<br><b>Level = 1:</b> All commands that can be accessed by a user with privilege level between 1 and 6 inclusive<br><b>Level = 7:</b> All commands that can be accessed by a user with privilege level between 7 and 14 inclusive<br><b>Level = 15:</b> All commands that can be accessed by a user with privilege level 15 |
| group             | Specify the server group where authorization messages are sent. Only the <code>tacacs+</code> group is available for this command.                                                                                                                                                                                                                                                                                                                                                              |
| tacacs+           | Use all TACACS+ servers configured by the <code>tacacs-server host</code> command.                                                                                                                                                                                                                                                                                                                                                                                                              |
| default           | Configure the default authorization commands method list.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <list-name>       | Configure a named authorization commands method list                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| none              | If specified, this provides a local fallback to command authorization so that if authorization servers become unavailable then the device will accept all commands normally allowed for the privilege level of the user.                                                                                                                                                                                                                                                                        |

**Mode** Global Configuration

**Usage notes** TACACS+ command authorization provides centralized control of the commands available to a user of an AlliedWare Plus device. Once enabled:

- The command string and username are encrypted and sent to the first available configured TACACS+ server (the first server configured) for authorization.

- The TACACS+ server decides if the user is authorized to execute the command and returns the decision to the AlliedWare Plus device.
- Depending on this decision the device will then either execute the command or notify the user that authorization has failed.

If multiple TACACS+ servers are configured, and the first server is unreachable or does not respond, the other servers will be queried, in turn, for an authorization decision. If all servers are unreachable and a local fallback has been configured, with the **none** parameter, then commands are authorized based on the user's privilege level; the same behavior as if command authorization had not been configured. If, however, the local fallback is not configured and all servers become unreachable then all commands except **logout**, **exit**, and **quit** will be denied.

The **default** method list is defined with a local fallback unless configured differently using this command.

**Example** To configure a commands authorization method list, named TAC15, using all TACACS+ servers to authorize commands for privilege level 15, with a local fallback, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authorization commands 15 TAC15 group
tacacs+ none
```

To configure the default method list to authorize commands for privilege level 7, with no local fallback, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authorization commands 7 default group
tacacs+
```

To remove the authorization method list TAC15, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authorization commands 15 TAC15
```

**Related commands** [aaa authorization config-commands](#)  
[authorization commands](#)  
[tacacs-server host](#)

**Command changes** Version 5.4.6-2.1: command added

# aaa authorization config-commands

**Overview** Use this command to enable command authorization on configuration mode commands. By default, command authorization applies to commands in exec mode only.

Use the **no** variant of this command to disable command authorization on configuration mode commands.

**Syntax** `aaa authorization config-commands`  
`no aaa authorization config-commands`

**Default** By default, command authorization is disabled on configuration mode commands.

**Mode** Global Configuration

**Usage notes** If authorization of configuration mode commands is not enabled then all configuration commands are accepted by default, including command authorization commands.

**NOTE:** *Authorization of configuration commands is required for a secure TACACS+ command authorization configuration as it prevents the feature from being disabled to gain access to unauthorized exec mode commands.*

**Example** To enable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authorization config-commands
```

To disable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authorization config-commands
```

**Related commands** [aaa authorization commands](#)  
[authorization commands](#)  
[tacacs-server host](#)

**Command changes** Version 5.4.6-2.1: command added



# aaa group server

**Overview** Use this command to create an AAA group of RADIUS or LDAP servers, and to enter Server Group Configuration mode.

A server group is used to specify a subset of RADIUS or LDAP servers in AAA commands. Once in Server Group Configuration mode you can add servers to the group.

Use the **no** variant of this command to remove an existing server group.

**Syntax** `aaa group server {radius|ldap} <group-name>`  
`no aaa group server {radius|ldap} <group-name>`

| Parameter    | Description                                |
|--------------|--------------------------------------------|
| radius       | Create or configure a RADIUS server group. |
| ldap         | Create or configure an LDAP server group.  |
| <group-name> | Server group name.                         |

**Mode** Global Configuration

**Usage notes** To add servers to a RADIUS or LDAP server group, use the **server** command. Each RADIUS server in a server group must be configured using the [radius-server host](#) command. Similarly, each LDAP server in a server group must be configured using the [ldap-server](#) command.

Server groups named 'radius' and 'ldap' are predefined and include all RADIUS and LDAP servers configured using the [radius-server host](#) or [ldap-server](#) commands.

**Examples** To create a RADIUS server group named 'GROUP1' with hosts 192.168.1.1, 192.168.2.1 and 192.168.3.1, use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.2.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.3.1 auth-port 1812 acct-port 1813
```

To remove a RADIUS server group named 'GROUP1' from the configuration, use the command:

```
awplus(config)# no aaa group server radius GROUP1
```

To create an LDAP server group named 'GROUP2' with servers named 'SERVER1', 'SERVER2' and 'SERVER3', use the commands:

```
awplus(config)# aaa group server ldap GROUP2
awplus(config-ldap-group)# server SERVER1
awplus(config-ldap-group)# server SERVER2
awplus(config-ldap-group)# server SERVER3
```

To remove an LDAP server group named 'GROUP2' from the configuration, use the command:

```
awplus(config)# no aaa group server ldap GROUP2
```

**Related  
commands**

[aaa accounting login](#)  
[aaa authentication login](#)  
[ldap-server](#)  
[radius-server host](#)  
[server \(ldap-group\)](#)  
[server \(RADIUS server group\)](#)  
[show ldap server group](#)  
[show radius server group](#)

**Command  
changes**

Version 5.5.2-1.1: **ldap** parameter added

# aaa local authentication attempts lockout-time

**Overview** This command configures the duration of the user lockout period.

Use the **no** variant of this command to restore the duration of the user lockout period to its default of 300 seconds (5 minutes).

**Syntax** `aaa local authentication attempts lockout-time <lockout-time>`  
`no aaa local authentication attempts lockout-time`

| Parameter                         | Description                                                         |
|-----------------------------------|---------------------------------------------------------------------|
| <code>&lt;lockout-time&gt;</code> | <code>&lt;0-10000&gt;</code> . Time in seconds to lockout the user. |

**Mode** Global Configuration

**Default** The default for the lockout-time is 300 seconds (5 minutes).

**Usage notes** While locked out all attempts to login with the locked account will fail. The lockout can be manually cleared by another privileged account using the [clear aaa local user lockout](#) command.

**Examples** To configure the lockout period to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts lockout-time
600
```

To restore the default lockout period of 5 minutes (300 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# no aaa local authentication attempts
lockout-time
```

**Related commands** [aaa local authentication attempts max-fail](#)  
[aaa local authentication attempts max-fail remote-login-only](#)  
[clear aaa local user lockout](#)

# aaa local authentication attempts max-fail

**Overview** This command configures the maximum number of failed login attempts before a user account is locked out. Every time a login attempt fails the failed login counter is incremented.

Use the **no** variant of this command to restore the maximum number of failed login attempts to the default setting (five failed login attempts).

**Syntax** `aaa local authentication attempts max-fail <failed-logins>`  
`no aaa local authentication attempts max-fail`

| Parameter                          | Description                                                                             |
|------------------------------------|-----------------------------------------------------------------------------------------|
| <code>&lt;failed-logins&gt;</code> | <code>&lt;1-32&gt;</code> . Number of login failures allowed before locking out a user. |

**Mode** Global Configuration

**Default** The default for the maximum number of failed login attempts is five failed login attempts.

**Usage** When the failed login counter reaches the limit configured by this command that user account is locked out for a specified duration configured by the [aaa local authentication attempts lockout-time](#) command.

When a successful login occurs the failed login counter is reset to 0. When a user account is locked out all attempts to login using that user account will fail.

**Examples** To configure the number of login failures that will lock out a user account to two login attempts, use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts max-fail 2
```

To restore the number of login failures that will lock out a user account to the default number of login attempts (five login attempts), use the commands:

```
awplus# configure terminal
awplus(config)# no aaa local authentication attempts max-fail
```

**Related commands** [aaa local authentication attempts lockout-time](#)  
[aaa local authentication attempts max-fail remote-login-only](#)  
[clear aaa local user lockout](#)

# aaa local authentication attempts max-fail remote-login-only

**Overview** Use this command to configure account lockout to remote logins only. This means that console logins are not subject to lock out when this feature is configured.

This command allow users to login via the physical console port even when the account is locked due to reaching the maximum number of failed login attempts.

Use the **no** variant of this command to prevent users from logging in via the console port when the maximum number of failed login attempts is reached.

**Syntax** `aaa local authentication attempts max-fail remote-login-only`  
`no aaa local authentication attempts max-fail remote-login-only`

**Default** Not set. Max-fail lockout applies to all logins.

**Mode** Global Configuration

**Example** To configure account lock-out to remote login only, use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts max-fail
remote-login-only
```

To configure account lock-out to apply to all logins, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa local authentication attempts max-fail
remote-login-only
```

**Related commands** [aaa local authentication attempts max-fail](#)  
[aaa local authentication attempts lockout-time](#)  
[clear aaa local user lockout](#)

**Command changes** Version 5.5.4-1.2: command added

# aaa login fail-delay

**Overview** Use this command to configure the minimum time period between failed login attempts. This setting applies to login attempts via the console, SSH and Telnet. Use the **no** variant of this command to reset the minimum time period to its default value.

**Syntax** `aaa login fail-delay <1-10>`  
`no aaa login fail-delay`

| Parameter | Description                                                   |
|-----------|---------------------------------------------------------------|
| <1-10>    | The minimum number of seconds required between login attempts |

**Default** 1 second

**Mode** Global configuration

**Example** To apply a delay of at least 5 seconds between login attempts, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa login fail-delay 5
```

**Related commands** [aaa authentication login](#)  
[aaa local authentication attempts logout-time](#)  
[clear aaa local user logout](#)

# accounting login

**Overview** This command applies a login accounting method list to console or VTY lines for user login. When login accounting is enabled using this command, logging events generate an accounting record to the accounting server.

The accounting method list must be configured first using this command. If an accounting method list is specified that has not been created by this command then accounting will be disabled on the specified lines.

The **no** variant of this command resets AAA Accounting applied to console or VTY lines for local or remote login. **default** login accounting is applied after issuing the **no accounting login** command. Accounting is disabled with **default**.

**Syntax** `accounting login {default|<list-name>}`  
`no accounting login`

| Parameter   | Description                     |
|-------------|---------------------------------|
| default     | Default accounting method list. |
| <list-name> | Named accounting method list.   |

**Default** By default login accounting is disabled in the **default** accounting server. No accounting will be performed until accounting is enabled using this command.

**Mode** Line Configuration

**Examples** To apply the accounting server `USERS` to all VTY lines, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)# accounting login USERS
```

To reset accounting for login sessions on the console, use the following commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# no accounting login
```

**Related commands** [aaa accounting commands](#)  
[aaa accounting login](#)

# authorization commands

**Overview** This command applies a command authorization method list, defined using the [aaa authorization commands](#) command, to console and VTY lines.

Use the **no** variant of this command to reset the command authorization configuration on the console and VTY lines.

**Syntax** `authorization commands <privilege-level> {default|<list-name>}`  
`no authorization commands <privilege-level>`

| Parameter                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;privilege-level&gt;</code> | The privilege level of the set of commands the method list will be applied to.<br>AlliedWare Plus defines three sets of commands, that are indexed by a level value:<br><b>Level = 1:</b> All commands that can be accessed by a user with privilege level between 1 and 6 inclusive<br><b>Level = 7:</b> All commands that can be accessed by a user with privilege level between 7 and 14 inclusive<br><b>Level = 15:</b> All commands that can be accessed by a user with privilege level 15 |
| <code>default</code>                 | Configure the default authorization commands method list.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <code>&lt;list-name&gt;</code>       | Configure a named authorization commands method list                                                                                                                                                                                                                                                                                                                                                                                                                                            |

**Default** The **default** method list is applied to each console and VTY line by default.

**Mode** Line Configuration

**Usage notes** If the specified method list does not exist users will not be enable to execute any commands in the specified method list on the specified VTY lines.

**Example** To apply the TAC15 command authorization method list with privilege level 15 to VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# authorization commands 15 TAC15
```

To reset the command authorization configuration with privilege level 15 on VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# no authorization commands 15
```

**Related commands** [aaa authorization commands](#)



aaa authorization config-commands

tacacs-server host

**Command  
changes**

Version 5.4.6-2.1: command added

# clear aaa local user lockout

**Overview** Use this command to clear the lockout on a specific user account or all user accounts.

**Syntax** `clear aaa local user lockout {username <username>|all}`

| Parameter  | Description                           |
|------------|---------------------------------------|
| username   | Clear lockout for the specified user. |
| <username> | Specifies the user account.           |
| all        | Clear lockout for all user accounts.  |

**Mode** Privileged Exec

**Examples** To unlock the user account 'bob' use the following command:

```
awplus# clear aaa local user lockout username bob
```

To unlock all user accounts use the following command:

```
awplus# clear aaa local user lockout all
```

**Related commands** [aaa local authentication attempts lockout-time](#)

# debug aaa

**Overview** This command enables AAA debugging.

Use the **no** variant of this command to disable AAA debugging.

**Syntax** `debug aaa [accounting|all|authentication|authorization]`  
`no debug aaa [accounting|all|authentication|authorization]`

| Parameter      | Description                        |
|----------------|------------------------------------|
| accounting     | Accounting debugging.              |
| all            | All debugging options are enabled. |
| authentication | Authentication debugging.          |
| authorization  | Authorization debugging.           |

**Default** AAA debugging is disabled by default.

**Mode** Privileged Exec

**Examples** To enable authentication debugging for AAA, use the command:

```
awplus# debug aaa authentication
```

To disable authentication debugging for AAA, use the command:

```
awplus# no debug aaa authentication
```

**Related commands** [show debugging aaa](#)  
[undebug aaa](#)

# login authentication

**Overview** Use this command to apply an AAA server for authenticating user login attempts from a console or remote logins on these console or VTY lines. The authentication method list must be specified by the **aaa authentication login** command. If the method list has not been configured by the **aaa authentication login** command, login authentication will fail on these lines.

Use the **no** variant of this command to reset AAA Authentication configuration to use the default method list for login authentication on these console or VTY lines.

**Command Syntax** login authentication {default|<list-name>}  
no login authentication

| Parameter   | Description                                                                                                                                                                                                        |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| default     | The default authentication method list. If the default method list has not been configured by the <a href="#">aaa authentication login</a> command, the local user database is used for user login authentication. |
| <list-name> | Named authentication server.                                                                                                                                                                                       |

**Default** The default login authentication method list, as specified by the [aaa authentication login](#) command, is used to authenticate user login. If this has not been specified, the default is to use the local user database.

**Mode** Line Configuration

**Examples** To apply the authentication method list called `CONSOLE` to the console port terminal line (asyn 0), use the following commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# login authentication CONSOLE
```

To reset user authentication configuration on all VTY lines, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)# no login authentication
```

**Related commands** [aaa authentication login](#)  
[line](#)

# proxy-port

**Overview** Use this command to change the local UDP port used for communication between local RADIUS client applications and the RadSecProxy AAA application. Any unused UDP port may be selected. The default port is 1645.

Use the **no** variant of this command to change the UDP port back to the default of 1645.

**Syntax** `proxy-port <port>`  
`no proxy-port`

| Parameter                 | Description               |
|---------------------------|---------------------------|
| <code>&lt;port&gt;</code> | UDP Port Number, 1-65536. |

**Default** The default port is 1645.

**Mode** RadSecProxy AAA Configuration Mode

**Usage notes** It is not necessary to change the value from the default unless UDP port 1645 is required for another purpose. RADIUS requests received on this port from external devices will be ignored. The port is only used for local (intra-device) communication.

**Example** To configure change the UDP port to 7001, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# proxy-port 7001
```

**Related commands** [radius-secure-proxy aaa](#)  
[server \(radsecproxy-aaa\)](#)  
[server name-check](#)  
[server trustpoint](#)

# radius-secure-proxy aaa

**Overview** Use this command to enter the RadSecProxy AAA (authentication, authorization, and accounting) application configuration mode. This application allows local RADIUS-based clients on system to communicate with remote RadSec servers via a secure (TLS) proxy.

**Syntax** `radius-secure-proxy aaa`

**Mode** Global Configuration Mode

**Example** To change mode from User Exec mode to the RadSecProxy AAA configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)#
```

**Related commands**

- [proxy-port](#)
- [server \(radsecproxy-aaa\)](#)
- [server name-check](#)
- [server trustpoint](#)

## server (radsecproxy-aaa)

**Overview** Use this command to add a server to the RadSecProxy AAA application. Local RADIUS client applications will attempt, via the proxy, to communicate with any RadSec servers that are operational (in addition to any non-TLS RADIUS servers that are configured).

Use the **no** variant of this command to delete a previously-configured server from the RadSecProxy AAA application.

**Syntax** `server {<hostname>|<ip-addr>} [timeout <1-1000>] [name-check {on|off}]`  
`no server {<hostname>|<ip-addr>}`

| Parameter  | Description                                                                                                                                                                     |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <hostname> | Hostname of RadSec server                                                                                                                                                       |
| <ip-addr>  | Specify the client IPv4 address, in dotted decimal notation (A.B.C.D).                                                                                                          |
| timeout    | Specify the amount of time that the RadSecProxy AAA application should wait for replies from this server. RADIUS server timeout (which defaults to 5 seconds).                  |
| <1-1000>   | Time in seconds to wait for a server reply.                                                                                                                                     |
| name-check | Specify whether or not to enforce certificate name checking for this client. If the parameter is not specified then the global behavior, which defaults to <b>on</b> , is used. |
|            | <code>on</code> Enable name checking for this client.                                                                                                                           |
|            | <code>off</code> Disable name checking for this client.                                                                                                                         |

**Mode** RadSecProxy AAA Configuration Mode

**Usage notes** The server may be specified by its domain name or by its IPv4 address. If a domain name is used, it must be resolvable using a configured DNS name server.

Each server may be configured with a timeout; if not specified, the global timeout value for RADIUS servers will be used. The global timeout may be changed using the **radius-server timeout** command. The default global timeout is 5 seconds.

Each server may be configured to use certificate name-checking; if not specified, the global behavior defined by **server name-check** or **no server name-check** will be used. If name checking is enabled, the Common Name portion of the subject field of the server's X.509 certificate must match the domain name or IP address specified in this command.

**Example** To add a server 'mynas.local' with a timeout of 3 seconds, and name checking off, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# server mynas.local name-check
off
```

**Related commands**

- [proxy-port](#)
- [radius-secure-proxy aaa](#)
- [server name-check](#)
- [server trustpoint](#)



# server mutual-authentication

**Overview** This command enables or disables mutual certificate authentication for all RadSecProxy servers. When enabled, the RadSecProxy AAA application will send a local X.509 certificate to the server when establishing a TLS connection.

Use the **no** variant of this command to disable mutual certificate validation causing the RadSecProxy AAA application to not transmit a certificate to the server.

**NOTE:** *If mutual authentication is disabled on the client (AAA) application but enabled on the server, a connection will not be established.*

**Syntax** `server mutual-authentication`  
`no server mutual-authentication`

**Default** Mutual authentication is enabled by default.

**Mode** RadSecProxy AAA Configuration Mode

**Example** Disable mutual certificate validation with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# no server
mutual-authentication
```

**Related commands** [radius-secure-proxy aaa](#)  
[server name-check](#)  
[server \(radsecproxy-aaa\)](#)

**Command changes** Version 5.4.6-2.1: command added

# server name-check

**Overview** This command sets the global behavior for certificate name-checking for the RadSecProxy AAA application to **on**. This behavior will be used for all servers associated with the application that do not specify a behavior on a per-server basis. If name-checking is enabled, the Common Name portion of the subject field of the client's X.509 certificate must match the domain name or IP address specified in the **server (radsecproxy-aaa)** command.

Use the **no** variant of this command to set the global behavior for certificate name checking to **off**

**Syntax** `server name-check`  
`no server name-check`

**Default** Certificate name checking is on by default.

**Mode** RadSecProxy AAA Configuration Mode

**Example** Disable certificate name checking globally with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# no server name-check
```

**Related commands** [proxy-port](#)  
[radius-secure-proxy aaa](#)  
[server \(radsecproxy-aaa\)](#)  
[server trustpoint](#)

# server trustpoint

**Overview** This command adds one or more trustpoints to be used with the RadSecProxy AAA application. Multiple trustpoints may be specified, or the command may be executed more than once, to add multiple trustpoints to the application.

The **no** version of this command removes one or more trustpoints from the list of trustpoints associated with the application.

**Syntax** `server trustpoint [<trustpoint-list>]`  
`no server trustpoint [<trustpoint-list>]`

| Parameter         | Description                                             |
|-------------------|---------------------------------------------------------|
| <trustpoint-list> | Specify one or more trustpoints to be added or deleted. |

**Default** By default, no trustpoints are associated with the application.

**Mode** RadSecProxy AAA Configuration Mode

**Usage notes** The device certificate associated with first trustpoint added to the application will be transmitted to remote servers. The certificate received from the remote server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

If no trustpoints are specified in the command, the trustpoint list will be unchanged.

If **no server trustpoint** is issued without specifying any trustpoints, then all trustpoints will be disassociated from the application.

**Example** You can add multiple trustpoints to the RadSecProxy AAA application by executing the command multiple times:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# server trustpoint example_1
awplus(config-radsecproxy-aaa)# server trustpoint example_2
```

Alternatively, add multiple trustpoints with a single command:

```
awplus(config-radsecproxy-aaa)# server trustpoint example_3
example_4
```

Disassociate all trustpoints from the RadSecProxy AAA application using the command:

```
awplus(config-radsecproxy-aaa)# no server trustpoint
```

**Related commands** [proxy-port](#)  
[radius-secure-proxy aaa](#)

server (radsecproxy-aaa)  
server name-check

# show aaa local user locked

**Overview** This command displays the failed attempts against each user account attempting to login into the device, along with the failure times and locations.

Use this command's output to see if a user is currently locked out or not. You can check:

- the number of login attempts that have a 'V' in the 'Valid' column, and
- if the last attempt happened within the lockout time. If the number of 'V' attempts exceeds the maximum allowed number of attempts, and the last attempt is within the lockout time, then the user is locked out.

The maximum number of attempts is 5 by default. You can change it using the command **aaa local authentication attempts max-fail**. The lockout time is 5 minutes by default. You can change it using the command **aaa local authentication attempts lockout-time**.

Once a user's lockout status is cleared, this command will no longer display any failed attempts for that user. The status gets cleared by:

- being manually cleared by another privileged user, using the [clear aaa local user lockout](#) command, or
- the locked out user successfully logs into the system after waiting for the lockout time to pass.

In the Valid column:

- 'V' means this login attempt counts towards the maximum allowed number of attempts
- 'I' means this login attempt does not count towards the maximum allowed number of attempts, because it was more than 15 minutes ago.

**Syntax** `show aaa local user locked`

**Mode** User Exec and Privileged Exec

**Example** To display the current failed attempts for local users, use the command:

```
awplus# show aaa local user locked
```

**Output** Figure 34-1: Example output from the **show aaa local user locked** command

```
awplus#show aaa local user locked
```

| manager:            |       |             |       |
|---------------------|-------|-------------|-------|
| When                | Type  | Source      | Valid |
| 2023-02-09 11:48:15 | RHOST | 192.168.5.1 | V     |
| 2023-02-09 11:48:21 | RHOST | 192.168.5.1 | V     |
| user1:              |       |             |       |
| When                | Type  | Source      | Valid |
| 2023-02-09 11:47:28 | RHOST | 192.168.5.1 | V     |
| 2023-02-09 11:47:31 | TTY   | /dev/ttyS0  | V     |
| 2023-02-09 11:47:35 | TTY   | /dev/ttyS0  | V     |
| 2023-02-09 11:47:38 | RHOST | 192.168.5.1 | V     |
| 2023-02-09 11:47:49 | RHOST | 192.168.5.1 | V     |
| 2023-02-09 11:20:50 | TTY   | /dev/ttyS0  | I     |
| 2023-02-09 11:20:54 | RHOST | 192.168.5.1 | I     |
| 2023-02-09 11:47:19 | RHOST | 192.168.5.1 | V     |
| 2023-02-09 11:47:23 | TTY   | /dev/ttyS0  | V     |
| user2:              |       |             |       |
| When                | Type  | Source      | Valid |
| 2023-02-09 11:47:52 | TTY   | /dev/ttyS0  | V     |
| 2023-02-09 11:47:55 | RHOST | 192.168.5.1 | V     |
| 2023-02-09 11:47:58 | TTY   | /dev/ttyS0  | V     |
| 2023-02-09 11:48:05 | RHOST | 192.168.5.1 | V     |
| 2023-02-09 11:22:51 | RHOST | 192.168.5.1 | I     |
| 2023-02-09 11:22:54 | TTY   | /dev/ttyS0  | I     |
| user3:              |       |             |       |
| When                | Type  | Source      | Valid |
| 2023-02-09 11:38:58 | TTY   | /dev/ttyS0  | V     |
| 2023-02-09 11:39:04 | RHOST | 192.168.5.1 | V     |
| 2023-02-09 11:39:06 | TTY   | /dev/ttyS0  | V     |
| 2023-02-09 11:39:22 | RHOST | 192.168.5.1 | V     |
| 2023-02-09 11:39:26 | TTY   | /dev/ttyS0  | V     |

This output example was run at 11:49. The lockout-time and max-fail settings are set to their defaults:

- manager: is not locked out because they only have 2 valid attempts.
- user1: is locked out because they have 7 valid attempts and the most recent was within the lockout time.
- user2: is not locked out because only 4 attempts are valid.
- user3: is not locked out. Even though they have 5 valid attempts, the most recent attempt is older than the lockout time of 5 minutes.

**Related commands**

- [aaa local authentication attempts lockout-time](#)
- [aaa local authentication attempts max-fail](#)
- [clear aaa local user lockout](#)

# show aaa server group

**Overview** Use this command to list AAA users and any method lists applied to them.

**Syntax** show aaa server group

**Mode** Privileged Exec

**Example** To show the AAA configuration on a device, use the command:

```
awplus# show aaa server group
```

**Output** Figure 34-2: Example output from **show aaa server group**

|                              |           |         |        |            |       |
|------------------------------|-----------|---------|--------|------------|-------|
| awplus#show aaa server group |           |         |        |            |       |
| User                         | List Name |         | Method | Acct-Event |       |
| =====                        | =====     | =====   | =====  | =====      | ===== |
| login                        | auth      | default | -      | local      | -     |
| -----                        | -----     | -----   | -----  | -----      | ----- |
| cmd-1                        | auth      | -       | -      | -          | -     |
| -----                        | -----     | -----   | -----  | -----      | ----- |
| cmd-7                        | auth      | -       | -      | -          | -     |
| -----                        | -----     | -----   | -----  | -----      | ----- |
| cmd-15                       | auth      | -       | -      | -          | -     |
| -----                        | -----     | -----   | -----  | -----      | ----- |
| login                        | acct      | -       | -      | -          | -     |
| -----                        | -----     | -----   | -----  | -----      | ----- |
| openvpn                      | auth      | -       | -      | -          | -     |
| -----                        | -----     | -----   | -----  | -----      | ----- |
| isakmp                       | auth      | default | radius | group      | -     |
| -----                        | -----     | -----   | -----  | -----      | ----- |

# show debugging aaa

**Overview** Use this command to see what debugging is turned on for AAA (Authentication, Authorization, Accounting).

**Syntax** `show debugging aaa`

**Mode** User Exec and Privileged Exec

**Example** To display the current debugging status of AAA, use the command:

```
awplus# show debug aaa
```

**Output** Figure 34-3: Example output from the **show debug aaa** command

```
AAA debugging status:
Authentication debugging is on
Accounting debugging is off
```



# show radius server group

**Overview** Use this command to show the RADIUS server group configuration.

**Syntax** `show radius server group [<group-name>]`

| Parameter                       | Description               |
|---------------------------------|---------------------------|
| <code>&lt;group-name&gt;</code> | RADIUS server group name. |

**Default** Command name is set to something by default.

**Mode** Privileged Exec

**Usage** Use this command with the `<group-name>` parameter to display information for a specific RADIUS server group, or without the parameter to display information for all RADIUS server groups.

**Example** To display information for all RADIUS server groups, use the command:

```
awplus# show radius server group
```

To display a information for a RADIUS server group named 'rad\_group\_list1', use the command:

```
awplus# show radius server group rad_group_list1
```

**Output** Figure 34-4: Example output from **show radius server group**

```
awplus#show radius server group
RADIUS Group Configuration
 Group Name : radius?
 Server Host/ Auth Acct Auth Acct
 IP Address Port Port Status Status

 192.168.1.101 1812 1813 Active Active
 192.168.1.102 1812 1813 Active Active

 Group Name : rad_group_list1
 Server Host/ Auth Acct Auth Acct
 IP Address Port Port Status Status

 192.168.1.101 1812 1813 Active Active

 Group Name : rad_group_list2
 Server Host/ Auth Acct Auth Acct
 IP Address Port Port Status Status

 192.168.1.102 1812 1813 Active Active
```

Figure 34-5: Example output from **show radius server group rad\_group\_list1**

```
awplus#show radius server group rad_group_list1
RADIUS Group Configuration
 Group Name : rad_group_list1
 Server Host/ Auth Acct Auth Acct
 IP Address Port Port Status Status

 192.168.1.101 1812 1813 Active Active
```

**Related  
commands**

[aaa group server](#)

# undebbug aaa

**Overview** This command applies the functionality of the **no debug aaa** command.

# 35

# Lightweight Directory Access Protocol (LDAP) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure Lightweight Directory Access Protocol (LDAP).

LDAP is an authentication protocol that facilitates user access to various IT resources e.g. applications, servers, networking equipment, and file servers.

It can be used to connect to internal networks over OpenVPN. Although both LDAP and RADIUS are interchangeable on AlliedWare Plus devices as an authentication protocol, LDAP is added because of its ability to interact with directory services such as Microsoft's Active Directory (AD).

For more information, see the [LDAP Feature Overview and Configuration Guide](#).

- Command List**
- ["authentication \(ldap-server\)"](#) on page 1634
  - ["base-dn"](#) on page 1636
  - ["bind authenticate root-dn"](#) on page 1637
  - ["deadtime \(ldap-server\)"](#) on page 1638
  - ["debug ldap client"](#) on page 1639
  - ["group-attribute"](#) on page 1641
  - ["group-dn"](#) on page 1642
  - ["host \(ldap-server\)"](#) on page 1643
  - ["ldap-server"](#) on page 1645
  - ["login-attribute"](#) on page 1647
  - ["port \(ldap-server\)"](#) on page 1649
  - ["retransmit \(ldap-server\)"](#) on page 1650
  - ["search-filter"](#) on page 1651
  - ["secure cipher \(ldap-server\)"](#) on page 1653

- [“secure mode \(ldap-server\)”](#) on page 1655
- [“secure trustpoint \(ldap-server\)”](#) on page 1657
- [“server \(ldap-group\)”](#) on page 1658
- [“show ldap server group”](#) on page 1659
- [“timeout \(ldap-server\)”](#) on page 1661

# authentication (ldap-server)

**Overview** Use this command to set the authentication method used to authenticate users against the Lightweight Directory Access Protocol (LDAP) server.

Use the **no** variant of this command to reset the authentication method to **search**.

**Syntax** authentication {search|bind-only}  
no authentication

| Parameter | Description                                                                                                                                                                                                                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| search    | The <b>search</b> method initially binds to the LDAP server, then searches for the user, then binds to the user using the DN found with the search. The initial bind is either anonymous, or using the user specified with the <a href="#">bind authenticate root-dn</a> command.                                         |
| bind-only | The <b>bind-only</b> method attempts to bind to the LDAP server using a predicted DN based on the username, the user attribute (set with the login-attribute command) and the base DN (set with the <a href="#">base-dn</a> command). The format of this user DN is as follows: '<username>=<login-attribute>,<base-dn>'. |

**Default** Search

**Mode** LDAP Server Configuration

**Example** To set the authentication method to bind-only for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# authentication bind-only
```

To reset the authentication method to the default (search) for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no authentication
```

**Related commands** [base-dn](#)  
[bind authenticate root-dn](#)  
[ldap-server](#)  
[login-attribute](#)  
[search-filter](#)

**Command changes** Version 5.5.2-1.1: command added

# base-dn

- Overview** Use this command to set the base DN (Distinguished Name) of the LDAP server.
- When using 'search' authentication, the base DN is the LDAP server's starting point to search for the user within the directory.
- If 'bind-only' authentication is enabled, then the base DN is the suffix of the DN that is used to bind to the user.
- Use the **no** variant of this command to remove the configured base DN.

**Syntax** base-dn <base-dn>  
no base-dn

| Parameter | Description                     |
|-----------|---------------------------------|
| <base-dn> | The base DN of the LDAP server. |

**Default** Not set

**Mode** LDAP Server Configuration

**Example** To set the base DN for the LDAP server called 'Server1' to 'dc=example, dc=com', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# base-dn dc=example,dc=com
```

To clear the base DN for Server1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no base-dn
```

**Related commands**

- [authentication \(ldap-server\)](#)
- [bind authenticate root-dn](#)
- [group-attribute](#)
- [group-dn](#)
- [ldap-server](#)
- [login-attribute](#)
- [search-filter](#)

**Command changes** Version 5.5.2-1.1: command added



# bind authenticate root-dn

**Overview** Use this command to set the authenticated user to bind to when searching for a user on an LDAP server. Do not set this option if you wish to use anonymous binding with the 'search' method.

This option is ignored with the 'bind-only' authentication method.

Use the **no** variant of this command to unset the authenticated user.

**Syntax** `bind authenticate root-dn <user-dn> password <password>`  
`no bind authenticate root-dn`

| Parameter                     | Description                                  |
|-------------------------------|----------------------------------------------|
| <code>&lt;user-dn&gt;</code>  | The DN of the authenticated user to bind to. |
| <code>&lt;password&gt;</code> | The password of the authenticated user.      |

**Default** Not set

**Mode** LDAP Server Configuration

**Example** To set the authenticated user to 'cn=admin,dc=example,dc=com' with the password '12345678' for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# bind authenticate root-dn
cn=admin,dc=example,dc=com password 12345678
```

**Related commands** [authentication \(ldap-server\)](#)  
[base-dn](#)

[group-attribute](#)

[ldap-server](#)

[login-attribute](#)

[search-filter](#)

**Command changes** Version 5.5.2-1.1: command added

# deadtime (ldap-server)

**Overview** Use this command to configure the deadtime for an LDAP server. The configured deadtime is how long in seconds before an unresponsive LDAP server is considered dead.

Use the **no** variant of this command to remove the deadtime configured on an LDAP server. When you remove the deadtime, the server will never be considered dead.

**Syntax** `deadtime <0-1440>`  
`no deadtime`

| Parameter                   | Description                                                                                 |
|-----------------------------|---------------------------------------------------------------------------------------------|
| <code>&lt;0-1440&gt;</code> | The number of seconds that the server can be unresponsive for before it is considered dead. |

**Default** 0 seconds (the LDAP server is never considered dead)

**Mode** LDAP Server Configuration

**Example** To set the deadtime to 20 seconds for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# deadtime 20
```

To reset the deadtime to the default for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no deadtime
```

**Related commands** [host \(ldap-server\)](#)  
[ldap-server](#)  
[port \(ldap-server\)](#)  
[retransmit \(ldap-server\)](#)  
[show ldap server group](#)  
[timeout \(ldap-server\)](#)

**Command changes** Version 5.5.2-1.1: command added

# debug ldap client

**Overview** Use this command to enable LDAP debugging.

Use the **no** variant of this command to disable all LDAP debugging.

**Syntax**

```
debug ldap client all
debug ldap client {[acl] [args] [ber] [config] [conns] [filter]
[packets] [parse] [shell] [stats] [stats2] [sync] [trace]}
no debug ldap client
```

| Parameter | Enable or disable debugging for ...                       |
|-----------|-----------------------------------------------------------|
| all       | All LDAP debugging options                                |
| args      | Heavy trace debugging (args, arguments)                   |
| ber       | Print out packets sent and received (ber, Bit Error Rate) |
| config    | Configuration processing                                  |
| conns     | Connection management                                     |
| filter    | Search filter processing                                  |
| packets   | Debug packet handling                                     |
| parse     | Parsing processing                                        |
| shell     | Print communication with shell backends                   |
| stats     | Stats from connections, operations and results            |
| stats2    | Stats from log entries sent                               |
| sync      | Syncrepl consumer processing (LDAP Sync replication)      |
| trace     | Trace function calls                                      |

**Default** By default, all LDAP debugging is disabled.

**Mode** Global Configuration

**Example** To turn on all LDAP debugging, use the command:

```
awplus# debug ldap client all
```

To turn on filter and packet LDAP debugging, use the command:

```
awplus# debug ldap client filter packets
```

To disable all LDAP debugging, use the command:

```
awplus# no debug ldap client
```

**Related commands** [aaa authentication login](#)  
[aaa authentication openvpn](#)

aaa group server

ldap-server

**Command changes** Version 5.5.2-1.1: command added

# group-attribute

**Overview** Use this command to configure the name of the attribute that group members are stored in.

It is only necessary to set this option if [group-dn](#) is used and you don't want to use the default attribute, which is 'uniquemember'.

Use the **no** variant of this command to revert to the default group attribute.

**Syntax** `group-attribute <attribute>`  
`no group-attribute`

| Parameter                      | Description                                     |
|--------------------------------|-------------------------------------------------|
| <code>&lt;attribute&gt;</code> | The attribute that group members are stored in. |

**Default** The default group attribute is 'uniquemember'.

**Mode** LDAP Server Configuration

**Example** To set the group attribute for the LDAP server called 'Server1' to 'member', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# group-attribute member
```

To reset the group attribute to default for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no group-attribute
```

**Related commands** [base-dn](#)  
[bind authenticate root-dn](#)  
[group-dn](#)  
[ldap-server](#)  
[login-attribute](#)  
[search-filter](#)

**Command changes** Version 5.5.2-1.1: command added

# group-dn

**Overview** Use this command to configure the group DN (Distinguished Name) of the group that users should be a member of.

By default the device will determine this by checking the 'uniquemember' attribute of the group to see if it contains the user's DN string. This can be changed with the [group-attribute](#) command.

Use the **no** variant of this command to remove the configured group DN.

**Syntax** `group-dn <group-dn>`  
`no group-dn`

| Parameter                     | Description                                           |
|-------------------------------|-------------------------------------------------------|
| <code>&lt;group-dn&gt;</code> | The DN of the group that users should be a member of. |

**Default** Not set

**Mode** LDAP Server Configuration

**Example** To set the group DN for the LDAP server called 'Server1' to 'cn=Users,dc=example,dc=com', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# group-dn cn=Users,dc=example,dc=com
```

To clear the group DN for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no group-dn
```

**Related commands** [base-dn](#)  
[bind authenticate root-dn](#)  
[group-attribute](#)  
[ldap-server](#)  
[login-attribute](#)  
[search-filter](#)

**Command changes** Version 5.5.2-1.1: command added

# host (ldap-server)

**Overview** Use this command to configure the address of the remote LDAP server you want to connect to.

Use the **no** variant of this command to remove the remote LDAP server.

**Syntax** `host {<host-name>|<ip-address>|<ipv6-address>}`  
`no host`

| Parameter                         | Description                                                    |
|-----------------------------------|----------------------------------------------------------------|
| <code>&lt;hostname&gt;</code>     | The hostname of the LDAP server.                               |
| <code>&lt;ip-address&gt;</code>   | The IPv4 address of the LDAP server. Uses the format A.B.C.D.  |
| <code>&lt;ipv6-address&gt;</code> | The IPv6 address of the LDAP server. Uses the format x:x::x:x. |

**Default** Not set

**Mode** LDAP Server Configuration

**Example** To set the host for the LDAP server called 'Server1' to the IP address 10.0.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# host 10.0.0.1
```

To set the host for Server1 to the IPv6 address 2001:0db8::a2, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# host 2001:db8::a2
```

To set the host for Server1 to the hostname www.ldapserver.com, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# host www.ldapserver.com
```

To unset the host for Server1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no host
```

**Related commands** [ldap-server](#)  
[port \(ldap-server\)](#)

retransmit (ldap-server)  
secure mode (ldap-server)  
secure cipher (ldap-server)  
show ldap server group  
secure trustpoint (ldap-server)  
timeout (ldap-server)

**Command changes** Version 5.5.2-1.1: command added



# ldap-server

**Overview** Use this command to configure an LDAP server and enter LDAP server configuration mode.

Use the **no** variant of this command to remove the specified server.

**Syntax** `ldap-server <server-name>`  
`no ldap-server <server-name>`

| Parameter                        | Description                  |
|----------------------------------|------------------------------|
| <code>&lt;server-name&gt;</code> | The name of the LDAP server. |

**Default** Not set

**Mode** Global Configuration

**Example** To create and configure an LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)#
```

To configure the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)#
```

To remove an LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# no ldap-server Server1
```

**Related commands**

- [authentication \(ldap-server\)](#)
- [host \(ldap-server\)](#)
- [port \(ldap-server\)](#)
- [retransmit \(ldap-server\)](#)
- [secure cipher \(ldap-server\)](#)
- [secure mode \(ldap-server\)](#)
- [secure trustpoint \(ldap-server\)](#)
- [show ldap server group](#)
- [timeout \(ldap-server\)](#)

**Command changes** Version 5.5.2-1.1: command added

# login-attribute

**Overview** Use this command to set the name of the attribute user names are stored in. The device will search this attribute for the user's DN (Distinguished Name).

It is only necessary to set this option if you don't want to use the default attribute, which is 'uid'.

If the authentication method is 'bind-only', then this attribute is used as the first component of the user DN, with the base DN added to complete the user DN.

Use the **no** variant of this command to reset the login attribute to the default of 'uid'.

**Syntax** login-attribute <attribute>  
no login-attribute

| Parameter   | Description                                                     |
|-------------|-----------------------------------------------------------------|
| <attribute> | The LDAP attribute to use for the username of connecting users. |

**Default** uid

**Mode** LDAP Server Configuration

**Example** To set the login attribute for the LDAP server called 'Server1' to 'sAMAccountName', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# login-attribute sAMAccountName
```

To reset the login attribute for 'Server1' to the default, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no login-attribute
```

**Related command** [authentication \(ldap-server\)](#)  
[base-dn](#)  
[bind authenticate root-dn](#)  
[group-attribute](#)  
[group-dn](#)  
[ldap-server](#)  
[search-filter](#)

**Command changes** Version 5.5.2-1.1: command added

# port (ldap-server)

**Overview** Use this command to configure the port you are using to connect to the remote LDAP server.

Note that if secure ciphers are enabled, then the secure port is used instead. Secure ciphers are configured with the [secure mode \(ldap-server\)](#) command.

Use the **no** variant of this command to reset the port number to the default (389).

**Syntax** port <1-65535>  
no port

| Parameter | Description                       |
|-----------|-----------------------------------|
| <1-65535> | Port number from 1 through 65535. |

**Default** 389

**Mode** LDAP Server Configuration

**Example** To set the port for the LDAP server called 'Server1' to 1579, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# port 1579
```

To reset the port for 'Server1' to the default of 389, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no port
```

**Related commands**

- [deadtime \(ldap-server\)](#)
- [host \(ldap-server\)](#)
- [ldap-server](#)
- [retransmit \(ldap-server\)](#)
- [secure cipher \(ldap-server\)](#)
- [secure mode \(ldap-server\)](#)
- [secure trustpoint \(ldap-server\)](#)
- [show ldap server group](#)
- [timeout \(ldap-server\)](#)

**Command changes** Version 5.5.2-1.1: command added

# retransmit (ldap-server)

**Overview** Use this command to configure the number of times a device will attempt to reconnect to the LDAP server before aborting.

Use the **no** variant of this command to reset the reconnect attempts to the default value of 3.

**Syntax** `retransmit <0-100>`  
`no retransmit`

| Parameter                  | Description                                                                  |
|----------------------------|------------------------------------------------------------------------------|
| <code>&lt;0-100&gt;</code> | The number of times the device will attempt to reconnect to the LDAP server. |

**Default** 3 times

**Mode** LDAP Server Configuration

**Example** To set the number of reconnect attempts for the LDAP server called 'Server1' to 5 attempts, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# retransmit 5
```

To reset the number of reconnect attempts for 'Server1' to 3 attempts, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no retransmit
```

**Related commands** [deadtime \(ldap-server\)](#)  
[host \(ldap-server\)](#)  
[ldap-server](#)  
[port \(ldap-server\)](#)  
[timeout \(ldap-server\)](#)

**Command changes** Version 5.5.2-1.1: command added

# search-filter

**Overview** Use this command to add a filter to use when searching for a user on the LDAP server.

The filter should be a form similar to 'attribute=value' or '&(attribute1=value1)(attribute2=value2)

Use the **no** variant of this command to remove the search filter.

**Syntax** `search-filter <filter>`  
`no search-filter`

| Parameter                   | Description                                  |
|-----------------------------|----------------------------------------------|
| <code>&lt;filter&gt;</code> | The filter to use when searching for a user. |

**Default** Not set

**Mode** LDAP Server Configuration

**Usage notes** If the 'bind-only' authentication method is used, then this value is unused.  
For the search authentication method, a search operation is used to search the LDAP server. The client specifies the starting point (base DN) of the search, the search scope (either the object, its children, or the subtree rooted at the object), and a search filter.

**Example** To set a search filter on the LDAP server called 'Server1' to 'building=block1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# search-filter building=block1
```

To unset the search filter of 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no search-filter
```

**Related commands** [authentication \(ldap-server\)](#)  
[base-dn](#)  
[bind authenticate root-dn](#)  
[group-attribute](#)  
[group-dn](#)  
[ldap-server](#)

## login-attribute

**Command changes** Version 5.5.2-1.1: command added



# secure cipher (ldap-server)

**Overview** Use this command to configure the OpenSSL ciphers used in LDAP secure mode. You can choose groups of ciphers from a number of Mozilla TLS configs, or specify multiple individual ciphers in OpenSSL format.

Use the **no** variant of this command to remove the configured ciphers on a server.

**Syntax** `secure cipher {old|intermediate|modern}`  
`secure cipher <cipher-list>`  
`no secure cipher`

| Parameter     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| old           | Ciphers in Mozilla's old TLS config. Alongside the modern and intermediate ciphers, this includes the following ciphers:<br>DHE-RSA-CHACHA20-POLY1305,ECDHE-ECDSA-AES128SHA256,<br>ECDHE-RSA-AES128-SHA256,ECDHE-ECDSA-AES128-SHA,<br>ECDHE-RSA-AES128-SHA,ECDHE-ECDSA-AES256-SHA384,<br>ECDHE-RSA-AES256-SHA384, ECDHE-ECDSA-AES256-SHA,<br>ECDHE-RSA-AES256-SHA,DHE-RSA-AES128-SHA256, DHE-RSA-AES256-SHA256,<br>AES128-GCM-SHA256, AES256-GCM-SHA384,AES128-SHA256, AES256-SHA256,<br>AES128-SHA, AES256-SHA, DES-CBC3-SHA |
| intermediate  | Ciphers in Mozilla's intermediate TLS config. Alongside the modern ciphers, this includes the following ciphers:<br>ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-RSA-AES128-CM-SHA256,<br>ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-CM-SHA384,<br>ECDHE-ECDSA-CHACHA20-POLY1305,ECDHE-RSA-CHACHA20-POLY1305,<br>DHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES256-GCM-SHA384                                                                                                                                                               |
| modern        | Ciphers in Mozilla's modern TLS config. Includes the following ciphers:<br>TLS_AES_128_GCM_SHA256,TLS_AES_256_GCM_SHA384,<br>TLS_CHACHA20_POLY1305_SHA256                                                                                                                                                                                                                                                                                                                                                                     |
| <cipher-list> | The name (or names) of a cipher in OpenSSL format. This is a <b>space</b> separated list of cipher names, for example:<br>DHE-DSS-AES256-GCM-SHA384 TLS_AES_256_GCM_SHA384                                                                                                                                                                                                                                                                                                                                                    |

**Default** Not set

**Mode** LDAP Server Configuration

**Example** To use the Intermediate Mozilla cipher suite on the LDAP server called Server1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure cipher intermediate
```

To remove the configured ciphers on 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no secure cipher
```

To use the ciphers DHE-DSS-AES256-GCM-SHA384 and TLS\_AES\_256\_GCM\_SHA384 on 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure cipher
DHE-DSS-AES256-GCM-SHA384 TLS_AES_256_GCM_SHA384
```

**Related  
commands**

[host \(ldap-server\)](#)  
[ldap-server](#)  
[port \(ldap-server\)](#)  
[secure mode \(ldap-server\)](#)  
[secure trustpoint \(ldap-server\)](#)

**Command  
changes**

Version 5.5.2-1.1: command added

## secure mode (ldap-server)

**Overview** Use this command to configure the LDAP server to use secure mode. Secure mode encrypts communications with the LDAP server using TLS (Transport Layer Security). If you don't specify a port number, the default port (636) is used.

For secure mode, you should also set the CA certificate using the [secure trustpoint \(ldap-server\)](#) command.

Use **no secure mode** to disable secure mode for communicating with this LDAP server.

Use **no secure mode secure-port** to reset the secure mode port to the default.

**Syntax** secure mode [secure-port <port>]  
no secure mode  
no secure mode secure-port

| Parameter | Description                                            |
|-----------|--------------------------------------------------------|
| <port>    | The secure port for communicating with the LDAP server |

**Default** Secure mode is disabled, and the default port is 636

**Mode** LDAP Server Configuration

**Example** To enable secure mode for communicating with the LDAP server called 'Server1', with the default port, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure mode
```

To disable secure mode for communicating with 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no secure mode
```

To enable secure mode with the port 1234 for communicating with 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure mode secure-port 1234
```

To reset the secure mode port to the default on 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no secure mode secure-port
```

**Related  
commands**

[host \(ldap-server\)](#)  
[ldap-server](#)  
[port \(ldap-server\)](#)  
[secure cipher \(ldap-server\)](#)  
[secure trustpoint \(ldap-server\)](#)

**Command  
changes**

Version 5.5.2-1.1: command added

# secure trustpoint (ldap-server)

**Overview** Use this command to link a preconfigured trustpoint to the LDAP server configuration. The trustpoint must be the LDAP server certificate and is required to successfully connect to the LDAP server when secure mode is enabled.

Use the **no** variant of this command to remove a trustpoint from an LDAP server.

**Syntax** `secure trustpoint <trustpoint>`  
`no secure trustpoint`

| Parameter                       | Description                                          |
|---------------------------------|------------------------------------------------------|
| <code>&lt;trustpoint&gt;</code> | The name of the trustpoint used for LDAP secure mode |

**Default** Not set

**Mode** LDAP Server Configuration

**Example** To set the trustpoint to Trustpoint1 for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap server Server1
awplus(config-ldap-server)# secure trustpoint Trustpoint1
```

To remove the trustpoint from 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap server Server1
awplus(config-ldap-server)# no secure trustpoint
```

**Related commands** [host \(ldap-server\)](#)  
[ldap-server](#)  
[port \(ldap-server\)](#)  
[secure cipher \(ldap-server\)](#)  
[secure mode \(ldap-server\)](#)

**Command changes** Version 5.5.2-1.1: command added

# server (ldap-group)

**Overview** Use this command to add an LDAP server to an LDAP server group.

The server is identified by the name of the server, which is created using the [ldap-server](#) command.

Use the **no** variant of this command to remove an LDAP server from an LDAP server group.

**Syntax** `server <server-name>`  
`no server <server-name>`

| Parameter                        | Description                                                                 |
|----------------------------------|-----------------------------------------------------------------------------|
| <code>&lt;server-name&gt;</code> | The name of the LDAP server group, specified when creating the LDAP server. |

**Default** By default, LDAP servers are only added to the default 'ldap' server group.

**Mode** LDAP Server Group Configuration

**Usage notes** The server is appended to the server list of the group, and the order of configuration determines the precedence of servers.

**Example** To add the LDAP server called 'Server1' to the LDAP server group called 'Group1', use the commands:

```
awplus# configure terminal
awplus(config)# aaa group server ldap Group1
awplus(config-ldap-group)# server Server1
```

To remove 'Server1' from 'Group1', use the commands:

```
awplus# configure terminal
awplus(config)# aaa group server ldap Group1
awplus(config-ldap-group)# no server Server1
```

**Related commands** [aaa authentication login](#)  
[aaa authentication openvpn](#)  
[aaa group server](#)  
[ldap-server](#)  
[show ldap server group](#)

**Command changes** Version 5.5.2-1.1: command added

# show ldap server group

**Overview** Use this command to display information about LDAP server groups, their servers and the status of those servers.

**Syntax** `show ldap server group [<group-name>]`

| Parameter                       | Description                        |
|---------------------------------|------------------------------------|
| <code>&lt;group-name&gt;</code> | The name of the LDAP server group. |

**Mode** Global Configuration

**Usage notes** If you specify a single group name, you will only see information relating to that specific server group. Otherwise, all LDAP server groups are shown, including the 'ldap' group that contains every LDAP server.

**Example** To show all server groups, use the command:

```
awplus# show ldap server group
```

To show the default LDAP group that includes all the LDAP servers, use the command:

```
awplus# show ldap server group ldap
```

To show a server group named 'CustomGroup1', use the command:

```
awplus# show ldap server group CustomGroup1
```

**Output** Figure 35-1: Example output from **show ldap server group**

LDAP Group Configuration

Group Name : ldap

| LDAP server name | Server Host/IP Address | Port | Status        |
|------------------|------------------------|------|---------------|
| server_one       | 10.1.1.1               | N/A  | Alive         |
| server_two       | 10.2.1.1               | N/A  | Dead (1 hour) |

Group Name : CustomGroup1

| LDAP server name | Server Host/IP Address | Port | Status |
|------------------|------------------------|------|--------|
| server_one       | 10.1.1.1               | N/A  | Alive  |

Group Name : CustomGroup2

| LDAP server name                  | Server Host/IP Address | Port | Status |
|-----------------------------------|------------------------|------|--------|
| No LDAP servers currently defined |                        |      |        |

**Related commands**

- [aaa authentication login](#)
- [aaa authentication openvpn](#)
- [aaa group server](#)

deadtime (ldap-server)

ldap-server

port (ldap-server)

server (ldap-group)

**Command changes** Version 5.5.2-1.1: command added



# timeout (ldap-server)

**Overview** Use this command to set the time to wait for a connection before reattempting to connect to the LDAP server.

Use the **no** variant of this command to reset the timeout back to the default value.

**Syntax** `timeout <1-1000>`  
`no timeout`

| Parameter                   | Description                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------|
| <code>&lt;1-1000&gt;</code> | The number of seconds to wait for a connection before reattempting to connect to the LDAP server. |

**Default** 5 seconds

**Mode** LDAP Server Configuration

**Example** To set the server timeout for the LDAP server called 'Server1' to 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# timeout 10
```

To set the server timeout for 'Server1' to the default, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no timeout
```

**Related commands** [deadtime \(ldap-server\)](#)

[host \(ldap-server\)](#)

[ldap-server](#)

[port \(ldap-server\)](#)

[retransmit \(ldap-server\)](#)

**Command changes** Version 5.5.2-1.1: command added

# 36

# RADIUS Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure the device as a RADIUS client.

For more information, see the [RADIUS Feature Overview and Configuration Guide](#).

- Command List**
- ["auth-mac-promiscuous"](#) on page 1663
  - ["deadtime \(RADIUS server group\)"](#) on page 1664
  - ["debug radius"](#) on page 1665
  - ["ip radius require-message-authenticator"](#) on page 1666
  - ["ip radius source-interface"](#) on page 1667
  - ["radius-server deadtime"](#) on page 1668
  - ["radius-server host"](#) on page 1669
  - ["radius-server key"](#) on page 1672
  - ["radius-server retransmit"](#) on page 1673
  - ["radius-server timeout"](#) on page 1675
  - ["server \(RADIUS server group\)"](#) on page 1677
  - ["show debugging radius"](#) on page 1679
  - ["show radius"](#) on page 1680
  - ["show radius local-server auth-mac-promiscuous"](#) on page 1683
  - ["undebug radius"](#) on page 1684

# auth-mac-promiscuous

**Overview** Use this command to enable promiscuous mode for MAC address authentication on a local RADIUS server.

Use the **no** variant of this command to disable MAC authentication promiscuous mode on a local RADIUS server.

**Syntax** `auth-mac-promiscuous`  
`no auth-mac-promiscuous`

**Default** Disabled.

**Mode** RADIUS Server Configuration

**Usage notes** In promiscuous mode, the RADIUS server will respond with an Access-Accept for any Access-Request with a Radius Service-Type attribute of 'Call-Check', when the supplicants credentials are NOT in the user database.

If the credentials do appear in the database, the behavior of the server is unchanged.

**Example** To disable MAC authentication promiscuous mode on a local RADIUS server, use the commands:

```
awplus# radius-server local
awplus(config-radsrv)# no auth-mac-promiscuous
```

**Related commands** [show radius local-server auth-mac-promiscuous](#)

**Command changes** Version 5.5.3-2.1: command added

# deadtime (RADIUS server group)

**Overview** Use this command to configure the **deadtime** parameter for the RADIUS server group. This command overrides the global dead-time configured by the [radius-server deadtime](#) command. The configured deadtime is the time period in minutes to skip a RADIUS server for authentication or accounting requests if the server is 'dead'. Note that a RADIUS server is considered 'dead' if there is no response from the server within a defined time period.

Use the **no** variant of this command to reset the deadtime configured for the RADIUS server group. If the global deadtime for RADIUS server is configured the value will be used for the servers in the group. The global deadtime for the RADIUS server is set to 0 minutes by default.

**Syntax** `deadtime <0-1440>`  
`no deadtime`

| Parameter                   | Description                |
|-----------------------------|----------------------------|
| <code>&lt;0-1440&gt;</code> | Amount of time in minutes. |

**Default** The deadtime is set to 0 minutes by default.

**Mode** RADIUS Server Group Configuration

**Usage** If the RADIUS server does not respond to a request packet, the packet is retransmitted the number of times configured for the **retransmit** parameter (after waiting for a **timeout** period to expire). The server is then marked 'dead', and the time is recorded. The **deadtime** parameter configures the amount of time to skip a dead server; if a server is dead, no request message is sent to the server for the **deadtime** period.

**Examples** To configure the deadtime for 5 minutes for the RADIUS server group 'GROUP1', use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1
awplus(config-sg)# deadtime 5
```

To remove the deadtime configured for the RADIUS server group 'GROUP1', use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no deadtime
```

**Related commands** [aaa group server](#)  
[radius-server deadtime](#)

# debug radius

**Overview** This command enables RADIUS debugging. If no option is specified, all debugging options are enabled.

Use the **no** variant of this command to disable RADIUS debugging. If no option is specified, all debugging options are disabled.

**Syntax** debug radius [packet|event|all]  
no debug radius [packet|event|all]

| Parameter | Description                                          |
|-----------|------------------------------------------------------|
| packet    | Debugging for RADIUS packets is enabled or disabled. |
| event     | Debugging for RADIUS events is enabled or disabled.  |
| all       | Enable or disable all debugging options.             |

**Default** RADIUS debugging is disabled by default.

**Mode** Privileged Exec

**Examples** To enable debugging for RADIUS packets, use the command:

```
awplus# debug radius packet
```

To enable debugging for RADIUS events, use the command:

```
awplus# debug radius event
```

To disable debugging for RADIUS packets, use the command:

```
awplus# no debug radius packet
```

To disable debugging for RADIUS events, use the command:

```
awplus# no debug radius event
```

**Related commands** [show debugging radius](#)  
[undebug radius](#)

# ip radius require-message-authenticator

**Overview** Use this command to configure the RADIUS client to reject unverified RADIUS packets. This means it will discard any received RADIUS Access-Accept, Access-Challenge, and Access-Reject packets that do not have a valid Message-Authenticator attribute.

Use the **no** variant of this command to allow the client to accept unverified RADIUS packets.

**Syntax** `ip radius require-message-authenticator`  
`no ip radius require-message-authenticator`

**Default** Disabled

**Mode** Global Configuration

**Example** To require Message-Authenticator attributes in responses from RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# ip radius require-message-authenticator
```

**Related commands** [nas message-authenticator \(radsvr\)](#)  
[radius-server host](#)  
[show radius local-server nas](#)

**Command changes** Version 5.5.4-2.3: command added

# ip radius source-interface

**Overview** This command configures the source IP address of every outgoing RADIUS packet to use a specific IP address or the IP address of a specific interface. If the specified interface is down or there is no IP address on the interface, then the source IP address of outgoing RADIUS packets depends on the interface the packets leave.

Use the **no** variant of this command to remove the source interface configuration. The source IP address in outgoing RADIUS packets will be the IP address of the interface from which the packets are sent.

**Syntax** `ip radius source-interface {<interface>|<ip-address>}`  
`no ip radius source-interface`

| Parameter                       | Description                                      |
|---------------------------------|--------------------------------------------------|
| <code>&lt;interface&gt;</code>  | Interface name.                                  |
| <code>&lt;ip-address&gt;</code> | IP address in the dotted decimal format A.B.C.D. |

**Default** Source IP address of outgoing RADIUS packets depends on the interface the packets leave.

**Mode** Global Configuration

**Examples** To configure all outgoing RADIUS packets to use the IP address of the interface "vlan1" for the source IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface vlan1
```

To configure the source IP address of all outgoing RADIUS packets to use 192.168.1.10, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface 192.168.1.10
```

To reset the source interface configuration for all outgoing RADIUS packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip radius source-interface
```

**Related commands** [radius-server host](#)

# radius-server deadtime

**Overview** Use this command to specify the global **deadtime** for all RADIUS servers. If a RADIUS server is considered dead, it is skipped for the specified deadtime. This command specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

Use the **no** variant of this command to reset the global deadtime to the default of 0 seconds, so that RADIUS servers are not skipped even if they are dead.

**Syntax** `radius-server deadtime <minutes>`  
`no radius-server deadtime`

| Parameter | Description                                                          |
|-----------|----------------------------------------------------------------------|
| <minutes> | RADIUS server deadtime in minutes in the range 0 to 1440 (24 hours). |

**Default** The default RADIUS deadtime configured on the system is 0 seconds.

**Mode** Global Configuration

**Usage** The RADIUS client considers a RADIUS server to be dead if it fails to respond to a request after it has been retransmitted as often as specified globally by the [radius-server retransmit](#) command or for the server by the [radius-server host](#) command. To improve RADIUS response times when some servers may be unavailable, set a **deadtime** to skip dead servers.

**Examples** To set the dead time of the RADIUS server to 60 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server deadtime 60
```

To disable the dead time of the RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server deadtime
```

**Related commands** [deadtime \(RADIUS server group\)](#)  
[radius-server host](#)  
[radius-server retransmit](#)



# radius-server host

**Overview** Use this command to specify a remote RADIUS server host for authentication or accounting, and to set server-specific parameters. The parameters specified with this command override the corresponding global parameters for RADIUS servers. This command specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination UDP port numbers.

This command adds the RADIUS server address and sets parameters to the RADIUS server. The RADIUS server is added to the running configuration after you issue this command. If parameters are not set using this command then common system settings are applied.

Use the **no** variant of this command to remove the specified server host as a RADIUS authentication and/or accounting server and set the destination port to the default RADIUS server port number (1812).

**Syntax** `radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>] [key <key-string>] [retransmit <0-100>] [timeout <1-1000>]`  
`no radius-server host {<host-name>|<ip-address>} [acct-port <0-65535>] [auth-port <0-65535>]`

| Parameter    | Description                                                                                                                                                                                                                      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <host-name>  | Server host name. The DNS name of the RADIUS server host.                                                                                                                                                                        |
| <ip-address> | The IP address of the RADIUS server host.                                                                                                                                                                                        |
| acct-port    | Accounting port. Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the server is not used for accounting. The default UDP port for accounting is 1813.                                       |
| <0-65535>    | UDP port number. (Accounting port number is set to (accounting port number is set to 1813 by default) Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the host is not used for accounting. |
| auth-port    | Authentication port. Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the server is not used for authentication. The default UDP port for authentication is 1812.                       |
| <0-65535>    | UDP port number (authentication port number is set to 1812 by default). Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the host is not used for authentication.                       |
| timeout      | Specifies the amount of time to wait for a response from the server. If this parameter is not specified the global value configured by the <b>radius-server timeout</b> command is used.                                         |

| Parameter    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-1000>     | Time in seconds to wait for a server reply (timeout is set to 5 seconds by default). The time interval (in seconds to wait for the RADIUS server to reply before retransmitting a request or considering the server dead. This setting overrides the global value set by the <b>radius-server timeout</b> command. If no timeout value is specified for this server, the global value is used.                                                                                                                                                                                                                      |
| retransmit   | Specifies the number of retries before skip to the next server. If this parameter is not specified the global value configured by the <b>radius-server retransmit</b> command is used.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <0-100>      | Maximum number of retries (maximum number of retries is set to 3 by default). The maximum number of times to resend a RADIUS request to the server, if it does not respond within the timeout interval, before considering it dead and skipping to the next RADIUS server. This setting overrides the global setting of the <b>radius-server retransmit</b> command. If no retransmit value is specified, the global value is used.                                                                                                                                                                                 |
| key          | Set shared secret key with RADIUS servers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <key-string> | Shared key string applied. Specifies the shared secret authentication or encryption key for all RADIUS communications between this device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the string are used.<br><br>If spaces are used in the string, do not enclose the string in quotation marks unless the quotation marks themselves are part of the key. This setting overrides the global setting of the <b>radius-server key</b> command. If no key value is specified, the global value is used. |

**Default** The RADIUS client address is not configured (null) by default. No RADIUS server is configured.

**Mode** Global Configuration

**Usage** Multiple **radius-server host** commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host. If there are multiple RADIUS servers for this client, use this command multiple times—once to specify each server.

If you specify a host without specifying the auth port or the acct port, it will by default be configured for both authentication and accounting, using the default UDP ports. To set a host to be a RADIUS server for authentication requests only, set the **acct-port** parameter to 0; to set the host to be a RADIUS server for accounting requests only, set the **auth-port** parameter to 0.

A RADIUS server is identified by IP address, authentication port and accounting port. A single host can be configured multiple times with different authentication or accounting ports. All the RADIUS servers configured with this command are included in the predefined RADIUS server group radius, which may be used by AAA authentication, authorization and accounting commands. The client transmits

(and retransmits, according to the **retransmit** and **timeout** parameters) RADIUS authentication or accounting requests to the servers in the order you specify them, until it gets a response.

**Examples** To add the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20
```

To set the secret key to 'mySecret' on the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 key mySecret
```

To delete the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host 10.0.0.20
```

To configure rad1.company.com for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad1.company.com acct-port 0
```

To remove the RADIUS server rad1.company.com configured for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host rad1.company.com
acct-port 0
```

To configure rad2.company.com for accounting only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad2.company.com auth-port 0
```

To configure 192.168.1.1 with authentication port 1000, accounting port 1001 and retransmit count 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 192.168.1.1 auth-port 1000
acct-port 1001 retransmit 5
```

**Related  
commands**

[aaa group server](#)  
[radius-server key](#)  
[radius-server retransmit](#)  
[radius-server timeout](#)

**Command  
changes**

Version 5.5.2-1.1: **vrf** parameter added for products that support VRF  
Version 5.4.9-2.1: **key-encrypted** parameter added

# radius-server key

**Overview** This command sets a global secret key for RADIUS authentication on the device. The shared secret text string is used for RADIUS authentication between the device and a RADIUS server.

Note that if no secret key is explicitly specified for a RADIUS server, the global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to reset the secret key to the default (null).

**Syntax** `radius-server key <key-string>`  
`no radius-server key`

| Parameter                       | Description                                          |
|---------------------------------|------------------------------------------------------|
| <code>&lt;key-string&gt;</code> | Shared secret among RADIUS server and 802.1X client. |

**Default** The RADIUS server secret key on the system is not set by default (null).

**Mode** Global Configuration

**Usage** Use this command to set the global secret key shared between this client and its RADIUS servers. If no secret key is specified for a particular RADIUS server using the **radius-server host** command, this global key is used.

After enabling AAA authentication with the **aaa authentication login** command, set the authentication and encryption key using the **radius-server key** command so the key entered matches the key used on the RADIUS server.

**Examples** To set the global secret key to **allied** for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server key allied
```

To set the global secret key to **secret** for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server key secret
```

To delete the global secret key for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server key
```

**Related commands** [radius-server host](#)

# radius-server retransmit

- Overview** This command sets the retransmit counter to use RADIUS authentication on the device. This command specifies how many times the device transmits each RADIUS request to the RADIUS server before giving up.
- This command configures the **retransmit** parameter for RADIUS servers globally. If the **retransmit** parameter is not specified for a RADIUS server by the **radius-server host** command then the global configuration set by this command is used for the server instead.
- Use the **no** variant of this command to reset the re-transmit counter to the default (3).

**Syntax** radius-server retransmit <retries>  
no radius-server retransmit

| Parameter | Description                                                                                                                                                                                                                                                                                                                                 |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <retries> | RADIUS server retries in the range <0-100>. The number of times a request is resent to a RADIUS server that does not respond, before the server is considered dead and the next server is tried. If no retransmit value is specified for a particular RADIUS server using the <b>radius-server host</b> command, this global value is used. |

**Default** The default RADIUS retransmit count on the device is 3.

**Mode** Global Configuration

**Examples** To set the RADIUS **retransmit** count to 1, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 1
```

To set the RADIUS **retransmit** count to the default (3), use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server retransmit
```

To configure the RADIUS **retransmit** count globally with 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 5
```

To disable retransmission of requests to a RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 0
```

**Related  
commands**   radius-server deadtime  
                  radius-server host

# radius-server timeout

**Overview** Use this command to specify the RADIUS global timeout value. This is how long the device waits for a reply to a RADIUS request before retransmitting the request, or considering the server to be dead. If no timeout is specified for the particular RADIUS server by the **radius-server host** command, it uses this global timeout value.

Note that this command configures the **timeout** parameter for RADIUS servers globally.

The **no** variant of this command resets the transmit timeout to the default (5 seconds).

**Syntax** `radius-server timeout <seconds>`  
`no radius-server timeout`

| Parameter                    | Description                                                                                                                                                                                                                                                               |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;seconds&gt;</code> | RADIUS server timeout in seconds in the range 1 to 1000. The global time in seconds to wait for a RADIUS server to reply to a request before retransmitting the request, or considering the server to be dead (depending on the <b>radius-server retransmit</b> command). |

**Default** The default RADIUS transmit timeout on the system is 5 seconds.

**Mode** Global Configuration

**Examples** To globally set the device to wait 20 seconds before retransmitting a RADIUS request to unresponsive RADIUS servers, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 20
```

To set the RADIUS **timeout** parameter to 1 second, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 1
```

To set the RADIUS **timeout** parameter to the default (5 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server timeout
```

To configure the RADIUS server **timeout** period globally with 3 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 3
```

To reset the global **timeout** period for RADIUS servers to the default, use the following command:

```
awplus# configure terminal
awplus(config)# no radius-server timeout
```

**Related  
commands**

[radius-server deadtime](#)  
[radius-server host](#)  
[radius-server retransmit](#)



## server (RADIUS server group)

**Overview** This command adds a RADIUS server to a server group in RADIUS Server Group Configuration mode. The RADIUS server should be configured by the [radius-server host](#) command.

The device adds each server to the end of the group's list of servers, so add the servers in order of priority. If you add a server and it is already in the list, it will be removed and then re-added to the end of the list.

The server is identified by IP address and authentication and accounting UDP port numbers. So a RADIUS server can have multiple entries in a group with different authentication and/or accounting UDP ports. The **auth-port** specifies the UDP destination port for authentication requests to the server. To disable authentication for the server, set **auth-port** to 0. If the authentication port is missing, the default port number is 1812. The **acct-port** specifies the UDP destination port for accounting requests to the server. To disable accounting for the server, set **acct-port** to 0. If the accounting port is missing, the default port number is 1813.

Use the **no** variant of this command to remove a RADIUS server from the server group.

**Syntax**

```
server {<hostname>|<ip-address>} [auth-port <0-65535>]
[acct-port <0-65535>]

no server {<hostname>|<ip-address>} [auth-port <0-65535>]
[acct-port <0-65535>]
```

| Parameter    | Description                                                                                                                                                                                                                                                            |
|--------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <hostname>   | Server host name                                                                                                                                                                                                                                                       |
| <ip-address> | Server IP address<br>The server is identified by IP address, authentication and accounting UDP port numbers. So a RADIUS server can have multiple entries in a group with different authentication and/or accounting UDP ports.                                        |
| auth-port    | Authentication port<br>The <b>auth-port</b> specifies the UDP destination port for authentication requests to the server. To disable authentication for the server, set <b>auth-port</b> to 0. If the authentication port is missing, the default port number is 1812. |
| <0-65535>    | UDP port number (default: 1812)                                                                                                                                                                                                                                        |
| acct-port    | Accounting port<br>The <b>acct-port</b> specifies the UDP destination port for accounting requests to the server. To disable accounting for the server, set <b>acct-port</b> to 0. If the accounting port is missing, the default port number is 1813.                 |
| <0-65535>    | UDP port number (default: 1813)                                                                                                                                                                                                                                        |

**Default** The default Authentication port number is 1812 and the default Accounting port number is 1813.

**Mode** RADIUS Server Group Configuration

**Usage notes** The RADIUS server to be added must be configured by the **radius-server host** command. In order to add or remove a server, the **auth-port** and **acct-port** parameters in this command must be the same as the corresponding parameters in the **radius-server host** command.

**Examples** To create a RADIUS server group 'RAD\_AUTH1' for authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_AUTH1
awplus(config-sg)# server 192.168.1.1 acct-port 0
awplus(config-sg)# server 192.168.2.1 auth-port 1000 acct-port 0
```

To create a RADIUS server group 'RAD\_ACCT1' for accounting, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_ACCT1
awplus(config-sg)# server 192.168.2.1 auth-port 0 acct-port 1001
awplus(config-sg)# server 192.168.3.1 auth-port 0
```

To remove server 192.168.3.1 from the existing server group 'GROUP1', use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no server 192.168.3.1
```

**Related commands**

- [aaa accounting login](#)
- [aaa authentication login](#)
- [aaa group server](#)
- [radius-server host](#)

# show debugging radius

**Overview** This command displays the current debugging status for the RADIUS servers.

**Syntax** `show debugging radius`

**Mode** User Exec and Privileged Exec

**Example** To display the current debugging status of RADIUS servers, use the command:

```
awplus# show debugging radius
```

**Output** Figure 36-1: Example output from the **show debugging radius** command

```
RADIUS debugging status:
RADIUS event debugging is off
RADIUS packet debugging is off
```

# show radius

**Overview** This command displays the current RADIUS server configuration and status.

**Syntax** show radius

**Mode** User Exec and Privileged Exec

**Example** To display the current status of RADIUS servers, use the command:

```
awplus# show radius
```

**Output** Figure 36-2: Example output from the **show radius** command showing RADIUS servers

```
RADIUS Global Configuration
Source Interface : not configured
Secret Key : secret
Timeout : 5 sec
Retransmit Count : 3
Deadtime : 20 min
Server Host : 192.168.1.10
Authentication Port : 1812
Accounting Port : 1813
Secret Key : secret
Timeout : 3 sec
Retransmit Count : 2
Server Host : 192.168.1.11
Authentication Port : 1812
Accounting Port : not configured

Server Name/ Auth Acct Auth Acct
IP Address Port Port Status Status

192.168.1.10 1812 1813 Alive Alive
192.168.1.11 1812 N/A Alive N/A
```

**Example** See the sample output below showing RADIUS client status and RADIUS configuration:

```
awplus# show radius
```

**Output** Figure 36-3: Example output from the **show radius** command showing RADIUS client status

```
RADIUS global interface name: awplus
 Secret key:
 Timeout: 5
 Retransmit count: 3
 Deadtime: 0

Server Address: 150.87.18.89
 Auth destination port: 1812
 Accounting port: 1813
 Secret key: swg
 Timeout: 5
 Retransmit count: 3
 Deadtime: 0
```

| Output Parameter    | Meaning                                                                                            |
|---------------------|----------------------------------------------------------------------------------------------------|
| Source Interface    | The interface name or IP address to be used for the source address of all outgoing RADIUS packets. |
| Secret Key          | A shared secret key to a radius server.                                                            |
| Timeout             | A time interval in seconds.                                                                        |
| Retransmit Count    | The number of retry count if a RADIUS server does not response.                                    |
| Deadtime            | A time interval in minutes to mark a RADIUS server as "dead".                                      |
| Interim-Update      | A time interval in minutes to send Interim-Update Accounting report.                               |
| Group Deadtime      | The deadtime configured for RADIUS servers within a server group.                                  |
| Server Host         | The RADIUS server hostname or IP address.                                                          |
| Authentication Port | The destination UDP port for RADIUS authentication requests.                                       |
| Accounting Port     | The destination UDP port for RADIUS accounting requests.                                           |

| Output Parameter | Meaning                                                                                                                                                                            |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auth Status      | The status of the authentication port.<br>The status ("dead", "error", or "alive") of the RADIUS authentication server and, if dead, how long it has been dead for.                |
|                  | Alive      The server is alive.                                                                                                                                                    |
|                  | Error      The server is not responding.                                                                                                                                           |
|                  | Dead      The server is detected as dead and it will not be used for deadtime period. The time displayed in the output shows the server is in dead status for that amount of time. |
|                  | Unknown   The server is never used or the status is unknown.                                                                                                                       |
| Acct Status      | The status of the accounting port.<br>The status ("dead", "error", or "alive") of the RADIUS accounting server and, if dead, how long it has been dead for.                        |

# show radius local-server auth-mac-promiscuous

**Overview** Use this command to show the status of the **auth-mac-promiscuous** command.

**Syntax** `show radius local-server auth-mac-promiscuous`

**Mode** User Exec

**Usage notes** In promiscuous mode, the RADIUS server will respond with an Access-Accept for any Access-Request with a Radius Service-Type attribute of 'Call-Check', when the supplicants credentials are NOT in the user database.

If the credentials do appear in the database, the behavior of the server is unchanged.

**Example** To display the status of the **auth-mac-promiscuous** command, use the command:

```
awplus# show radius local-server auth-mac-promiscuous
```

**Output** Figure 36-4: Example output from **show radius local-server auth-mac-promiscuous**

```
awplus#show radius local-server auth-mac-promiscuous
Auth-mac promiscuous mode: Disabled
...
```

**Related commands** [auth-mac-promiscuous](#)

**Command changes** Version 5.5.3-2.1: command added

# undebbug radius

**Overview** This command applies the functionality of the **no debug radius** command.



# 37

# Local RADIUS Server Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure the local RADIUS server on the device. For more information, see the [Local RADIUS Server Feature Overview and Configuration Guide](#).

- Command List**
- ["attribute \(radsrv-grp\)"](#) on page 1687
  - ["authentication"](#) on page 1689
  - ["client \(radsecproxy-srv\)"](#) on page 1690
  - ["client mutual-authentication"](#) on page 1692
  - ["client name-check"](#) on page 1693
  - ["client trustpoint"](#) on page 1694
  - ["clear radius local-server statistics"](#) on page 1695
  - ["copy fdb-radius-users \(to file\)"](#) on page 1696
  - ["copy local-radius-user-db \(from file\)"](#) on page 1698
  - ["copy local-radius-user-db \(to file\)"](#) on page 1699
  - ["crypto pki enroll local \(deleted\)"](#) on page 1700
  - ["crypto pki enroll local local-radius-all-users \(deleted\)"](#) on page 1701
  - ["crypto pki enroll local user \(deleted\)"](#) on page 1702
  - ["crypto pki export local pem \(deleted\)"](#) on page 1703
  - ["crypto pki export local pkcs12 \(deleted\)"](#) on page 1704
  - ["crypto pki trustpoint local \(deleted\)"](#) on page 1705
  - ["debug crypto pki \(deleted\)"](#) on page 1706
  - ["domain-style"](#) on page 1707
  - ["egress-vlan-id \(radsrv-grp\)"](#) on page 1708

- [“egress-vlan-name \(radsrv-grp\)”](#) on page 1709
- [“group \(radsrv\)”](#) on page 1710
- [“help radius-attribute”](#) on page 1711
- [“nas”](#) on page 1713
- [“nas message-authenticator \(radsrv\)”](#) on page 1714
- [“radius-secure-proxy local-server”](#) on page 1716
- [“radius-server local”](#) on page 1717
- [“server auth-port”](#) on page 1718
- [“server enable”](#) on page 1719
- [“server trustpoint \(radsrv\)”](#) on page 1720
- [“show radius local-server group”](#) on page 1722
- [“show radius local-server nas”](#) on page 1723
- [“show radius local-server statistics”](#) on page 1724
- [“show radius local-server trustpoint”](#) on page 1726
- [“show radius local-server user”](#) on page 1727
- [“user \(radsrv\)”](#) on page 1729
- [“vlan \(radsrv-grp\)”](#) on page 1731

# attribute (radsrv-grp)

**Overview** Use this command to define a RADIUS attribute for the local RADIUS server user group.

For a complete list of defined RADIUS attributes and values, see the [Local RADIUS Server Feature Overview and Configuration Guide](#).

When used with the **value** parameter the **attribute** command configures RADIUS attributes to the user group. If the specified attribute is already defined then it is replaced with the new value.

Use the **no** variant of this command to delete an attribute from the local RADIUS server user group.

**Syntax** `attribute [repeated] {<attribute-name>|<attribute-id>} <value>`  
`no attribute {<attribute-name>|<attribute-id>}`

| Parameter        | Description                                                                                                                                                                                  |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| repeated         | This optional parameter allows you to set multiple instances of the same attribute name or attribute ID.                                                                                     |
| <attribute-name> | RADIUS attribute name for standard attributes or Vendor-Specific attributes (see the <a href="#">Local RADIUS Server Feature Overview and Configuration Guide</a> for tables of attributes). |
| <attribute-id>   | RADIUS attribute numeric identifier for standard attributes.                                                                                                                                 |
| <value>          | RADIUS attribute value.                                                                                                                                                                      |

**Default** By default, no attributes are configured.

**Mode** Local RADIUS Server User Group Configuration

**Usage notes** For the Standard attributes, the attribute may be specified using either the attribute name, or its numeric identifier. For example, the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause 1
```

will produce the same results as the command:

```
awplus(config-radsrv-group)# attribute 49 1
```

In the same way, where the specific attribute has a pre-defined value, the parameter <value> may be substituted with the Value Name or with its numeric value, for example the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause
user-request
```

will produce the same results as the command:

```
awplus(config-radsrv-group)# attribute 49 1
```

or the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause 1
```

You can define more than one instance of an attribute name (or id) by using the **repeated** parameter. For example:

```
awplus(config-radsrv-group)# attribute repeated
Nas-filter-Rule "deny in tcp from any to 0.0.0.0/0 23"

awplus(config-radsrv-group)# attribute repeated
Nas-filter-Rule "deny in tcp from any to fe80::b1 23"
```

**Examples** To define the attribute name 'Service-Type' with Administrative User (6) to the RADIUS User Group 'Admin', use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# attribute Service-Type 6
```

To delete the attribute 'Service-Type' from the RADIUS User Group 'Admin', use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# no attribute Service-Type
```

To define multiple values for attribute 'NAS-Filter-Rule', use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group dynamicAcl
awplus(config-radsrv-group)# attribute repeated
NAS-Filter-Rule "deny in tcp from any to 0.0.0.0/0 23"

awplus(config-radsrv-group)# attribute repeated
NAS-Filter-Rule "deny in tcp from any to fe80::b1 23"
```

To delete a specific value from the attribute 'NAS-Filter-Rule', use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group dynamicAcl
awplus(config-radsrv-group)# no attribute NAS-Filter-Rule "deny
in tcp from any to 0.0.0.0/0 23"
```

**Related  
commands** [egress-vlan-id \(radsrv-grp\)](#)  
[egress-vlan-name \(radsrv-grp\)](#)  
[help radius-attribute](#)

**Command  
changes** Version 5.5.0-1.1: **repeated** parameter added

# authentication

**Overview** Use this command to enable the specified authentication methods on the local RADIUS server.

Use the **no** variant of this command to disable specified authentication methods on the local RADIUS server.

**Syntax** `authentication {mac|eapmd5|eaptls|peap}`  
`no authentication {mac|eapmd5|eaptls|peap}`

| Parameter | Description                            |
|-----------|----------------------------------------|
| mac       | Enable MAC authentication method.      |
| eapmd5    | Enable EAP-MD5 authentication method.  |
| eaptls    | Enable EAP-TLS authentication method.  |
| peap      | Enable EAP-PEAP authentication method. |

**Default** All authentication methods are enabled by default.

**Mode** RADIUS Server Configuration

**Examples** The following commands enable EAP-MD5 authentication methods on the local RADIUS server.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# authentication eapmd5
```

The following commands disable EAP-MD5 authentication methods on Local RADIUS server.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no authentication eapmd5
```

**Related commands** [server enable](#)  
[show radius local-server statistics](#)

# client (radsecproxy-srv)

**Overview** Use this command to add a RadSec client (for example, a NAS device) to the RadSecProxy local-server application. The application will accept RADIUS requests from all configured clients.

Use the **no** variant of this command to delete a previously-configured client from the RadSecProxy local-server application.

**Syntax** `client {<hostname>|<ip-addr>} [name-check {on|off}]`  
`no client {<hostname>|<ip-addr>}`

| Parameter  | Description                                                                                                                                                                     |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <hostname> | Hostname of client.                                                                                                                                                             |
| <ip-addr>  | Specify the client IPv4 address, in dotted decimal notation (A.B.C.D).                                                                                                          |
| name-check | Specify whether or not to enforce certificate name checking for this client. If the parameter is not specified then the global behavior, which defaults to <b>on</b> , is used. |
| on         | Enable name checking for this client.                                                                                                                                           |
| off        | Disable name checking for this client.                                                                                                                                          |

**Mode** RadSecProxy Local Server Configuration

**Usage notes** The client may be specified by its domain name or by its IPv4 address. If a domain name is used, it must be resolvable using a configured DNS name server.

Each client may be configured to use certificate name-checking; if not specified, the global behavior defined by **client name-check** or **no client name-check** will be used. If name checking is enabled, the Common Name portion of the subject field of the client's X.509 certificate must match the domain name or IP address specified in this command.

**NOTE:** If mutual authentication is disabled then this parameter has no effect, see the [client mutual-authentication](#) command.

**Example** To add a client called 'mynas.local' with certificate name checking **off**, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# client mynas.local name-check
off
```

**Related commands** [client mutual-authentication](#)  
[client name-check](#)

client trustpoint  
radius-secure-proxy local-server

# client mutual-authentication

**Overview** This command enables or disables mutual certificate authentication for all RadSecProxy clients. When enabled, the RadSecProxy local-server application will request and validate an X.509 certificate from the client when establishing a connection.

The **no** variant of this command disables mutual certificate validation. The local-server application will still transmit the local server certificate to the client, but will not expect or validate a certificate from the client.

**Syntax** `client mutual-authentication`  
`no client mutual-authentication`

**Default** Mutual authentication is enabled by default.

**Mode** RadSecProxy Local Server Configuration

**Example** Disable mutual certificate validation with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radius-secure-proxy)# no client
mutual-authentication
```

**Related commands** [client \(radsecproxy-srv\)](#)  
[client name-check](#)  
[radius-secure-proxy local-server](#)

**Command changes** Version 5.4.6-2.1: command added



# client name-check

**Overview** This command sets the global behavior for certificate name-checking for the RadSecProxy localserver application to **on**. This behavior will be used for all clients associated with the application that do not specify a behavior on a per-client basis. If name-checking is enabled, the Common Name portion of the subject field of the client's X.509 certificate must match the domain name or IP address specified in the **client (radsecproxy-aaa)** command.

Use the **no** variant of this command to set the global behavior for certificate name checking to **off**

**Syntax** `client name-check`  
`no client name-check`

**Default** Certificate name checking is on by default.

**Mode** RadSecProxy Local Server Configuration

**Example** Disable certificate name checking globally with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# no client name-check
```

**Related commands** [client \(radsecproxy-srv\)](#)  
[client trustpoint](#)  
[radius-secure-proxy local-server](#)

# client trustpoint

**Overview** This command adds one or more trustpoints to be used with the RadSecProxy local-server application. Multiple trustpoints may be specified, or the command may be executed more than once, to add multiple trustpoints to the application.

The **no** version of this command removes one or more trustpoints from the list of trustpoints associated with the application.

**Syntax** `client trustpoint [<trustpoint-list>]`  
`no client trustpoint [<trustpoint-list>]`

| Parameter         | Description                                             |
|-------------------|---------------------------------------------------------|
| <trustpoint-list> | Specify one or more trustpoints to be added or deleted. |

**Mode** RadSecProxy Local Server Configuration

**Usage notes** The device certificate associated with the first trustpoint added to the application will be transmitted to remote servers. The certificate received from the remote server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

If you enter **client trustpoint** without specifying a trustpoint, the trustpoint list will be unchanged.

If you enter **no client trustpoint** without specifying a trustpoint, all trustpoints will be disassociated from the application.

**Example** You can add multiple trustpoints to the RadSecProxy local-server by executing the command multiple times:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)# client trustpoint example_1
awplus(config-radsecproxy-srv)# client trustpoint example_2
```

Alternatively, add multiple trustpoints with a single command:

```
awplus(config-radsecproxy-srv)# client trustpoint example_3
example_4
```

Disassociate all trustpoints from the RadSecProxy local-server application using the command:

```
awplus(config-radsecproxy-srv)# no client trustpoint
```

**Related commands** [client \(radsecproxy-srv\)](#)  
[client name-check](#)  
[radius-secure-proxy local-server](#)

# clear radius local-server statistics

**Overview** Use this command to clear the statistics stored on the device for the local RADIUS server.

Use this command without any parameters to clear all types of local RADIUS server statistics.

**Syntax** `clear radius local-server statistics [nas|server|user]`

| Parameter | Description                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------|
| nas       | Clear the NAS (Network Access Server) statistics on the device. For example, clearing statistics stored for NAS server invalid passwords.    |
| server    | Clear the Local RADIUS Server statistics on the device. For example, clearing Local RADIUS Servers statistics for all failed login attempts. |
| user      | Clear the Local RADIUS Server user statistics. For example, clearing statistics stored for the number of successful user logins.             |

**Mode** Privileged Exec

**Usage** Refer to the sample output for the [show radius local-server statistics](#) for further information about the type of statistics each parameter option for this command clears. Both the **nas** and **server** parameters clear unknown username and invalid passwords statistics, while the **user** parameter clears the number of successful and failed logins for each local RADIUS server user.

**Examples** To clear the NAS (Network Access Server) statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics nas
```

To clear the local RADIUS server statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics server
```

To clear the local RADIUS server user statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics user
```

**Related commands** [show radius local-server statistics](#)

## copy fdb-radius-users (to file)

**Overview** Use this command to create a set of local RADIUS server users from MAC addresses in the local FDB. A local RADIUS server user created using this command can be used for MAC authentication.

**Syntax** `copy fdb-radius-users  
{local-radius-user-db|nvs|flash|debug|tftp|scp|  
fserver|<url>} [interface <port>] [vlan <vid>] [group <name>]  
[export-vlan [<radius-group-name>]]`

| Parameter            | Description                                                                                                          |
|----------------------|----------------------------------------------------------------------------------------------------------------------|
| local-radius-user-db | Copy the local RADIUS server users created to the local RADIUS server.                                               |
| nvs                  | Copy the local RADIUS server users created to NVS memory.                                                            |
| flash                | Copy the local RADIUS server users created to Flash memory.                                                          |
| debug                | Copy the local RADIUS server users created to debug.                                                                 |
| tftp                 | Copy the local RADIUS server users created to the TFTP destination.                                                  |
| scp                  | Copy the local RADIUS server users created to the SCP destination.                                                   |
| fserver              | Copy the local RADIUS server users created to the remote file server.                                                |
| <url>                | Copy the local RADIUS server users created to the specified URL.                                                     |
| interface <port>     | Copy only MAC addresses learned on a specified device port. Wildcards may be used when specifying an interface name. |
| vlan <vid>           | Copy only MAC addresses learned on a specified VLAN.                                                                 |
| group <name>         | Assign a group name to the local RADIUS server users created.                                                        |
| export-vlan          | Export VLAN ID assigned to exported FDB entry.                                                                       |
| <radius-group-name>  | Prefix for Radius group name storing VLAN ID                                                                         |

**Mode** Privileged Exec

**Usage notes** The local RADIUS server users created are written to a specified destination file in local RADIUS user CSV (Comma Separated Values) format. The local RADIUS server users can then be imported to a local RADIUS server using the [copy local-radius-user-db \(from file\)](#) command.

The name and password of the local RADIUS server users created use a MAC address, which can be used for MAC authentication.

This command does not copy a MAC address learned by the CPU or the management port.

This command can filter FDB entries by the interface name and the VLAN ID. When the interface name and the VLAN ID are specified, this command generates local RADIUS server users from only the MAC address learned on the specified interface and on the specified VLAN.

**Examples** To register the local RADIUS server users from the local FDB directly to the local RADIUS server, use the command:

```
awplus# copy fdb-radius-users local-radius-user-db
```

To register the local RADIUS server users from the interface port1.0.1 to the local RADIUS server, use the command:

```
awplus# copy fdb-radius-users local-radius-user-db interface
port1.0.1
```

To copy output generated as local RADIUS server user data from MAC addresses learned on vlan10 on interface port1.0.1 to the file radius-user.csv, use the command:

```
awplus# copy fdb-radius-users radius-user.csv interface
port1.0.1 vlan10
```

To copy output generated as local RADIUS server user data from MAC addresses learned on vlan10 on interface port1.0.1 to a file on the remote file server, use the command:

```
awplus# copy fdb-radius-users fserver interface port1.0.1
vlan10
```

**Related commands** [copy local-radius-user-db \(to file\)](#)  
[copy local-radius-user-db \(from file\)](#)

# copy local-radius-user-db (from file)

**Overview** Use this command to copy the Local RADIUS server user data from a file. The file, including the RADIUS user data in the file, must be in the CSV (Comma Separated Values) format.

You can select **add** or **replace** as the copy method. The **add** parameter option copies the contents of specified file to the local RADIUS server user database. If the same user exists then the old user is removed before adding a new user. The **replace** parameter option deletes all contents of the local RADIUS server user database before copying the contents of specified file.

**Syntax** `copy <source-url> local-radius-user-db [add|replace]`

| Parameter    | Description                                                           |
|--------------|-----------------------------------------------------------------------|
| <source-url> | URL of the source file.                                               |
| add          | Add file contents to local RADIUS server user database.               |
| replace      | Replace current local RADIUS server user database with file contents. |

**Default** When no copy method is specified with this command the **replace** option is applied.

**Mode** Privileged Exec

**Examples** To replace the current local RADIUS server user data to the contents of `http://datahost/ user.csv`, use the following command:

```
awplus# copy http://datahost/user.csv local-radius-user-db
```

To add the contents of `http://datahost/user.csv` to the current local RADIUS server user database, use the following command:

```
awplus# copy http://datahost/user.csv local-radius-user-db add
```

**Related commands** [copy fdb-radius-users \(to file\)](#)  
[copy local-radius-user-db \(to file\)](#)

## copy local-radius-user-db (to file)

**Overview** Use this command to copy the local RADIUS server user data to a file. The output file produced is CSV (Comma Separated Values) format.

**Syntax** `copy local-radius-user-db  
{nvs|flash|tftp|scp|<destination-url>}`

| Parameter         | Description                  |
|-------------------|------------------------------|
| nvs               | Copy to NVS memory.          |
| flash             | Copy to Flash memory.        |
| tftp              | Copy to TFTP destination.    |
| scp               | Copy to SCP destination.     |
| <destination-url> | URL of the Destination file. |

**Mode** Privileged Exec

**Example** Copy the current local RADIUS server user data to http://datahost/user.csv.  
`awplus# copy local-radius-user-db http://datahost/user.csv`

**Related commands** [copy fdb-radius-users \(to file\)](#)  
[copy local-radius-user-db \(from file\)](#)

# crypto pki enroll local (deleted)

**Overview** This command is no longer available. Please use the following command instead:

```
crypto pki enroll <trustpoint>
```

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.



# crypto pki enroll local local-radius-all-users (deleted)

**Overview** This command is no longer available. Please use the following command instead:

```
crypto pki enroll <trustpoint> local-radius-all-users
```

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

# crypto pki enroll local user (deleted)

**Overview** This command is no longer available. Please use the following command instead:

```
crypto pki enroll <trustpoint> user <username>
```

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

# crypto pki export local pem (deleted)

**Overview** This command is no longer available. Please use the [crypto pki export pem](#) command instead:

```
crypto pki export <trustpoint> pem [terminal|<url>]
```

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

# crypto pki export local pkcs12 (deleted)

**Overview** This command is no longer available. Please use the [crypto pki export pkcs12](#) command instead:

```
crypto pki export <trustpoint> pkcs12 {ca|server|<username>}
<url>
```

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

# crypto pki trustpoint local (deleted)

**Overview** This command is no longer available. Please use the following command instead:

```
crypto pki trustpoint <trustpoint>
```

Note that “local” is a valid name for a trustpoint, so you do not need to modify existing configurations or scripts.

# debug crypto pki (deleted)

**Overview** This command is no longer available.

# domain-style

**Overview** Use this command to enable a specified domain style on the local RADIUS server. The local RADIUS server decodes the domain portion of a username login string when this command is enabled.

Use the **no** variant of this command to disable the specified domain style on the local RADIUS server.

**Syntax** `domain-style {suffix-atsign|ntdomain}`  
`no domain-style {suffix-atsign|ntdomain}`

| Parameter                  | Description                                                    |
|----------------------------|----------------------------------------------------------------|
| <code>suffix-atsign</code> | Enable at sign "@" delimited suffix style, i.e. "user@domain". |
| <code>ntdomain</code>      | Enable NT domain style, i.e. "domain\user".                    |

**Default** This feature is disabled by default.

**Mode** RADIUS Server Configuration

**Usage notes** When both domain styles are enabled, the first domain style configured has the highest priority. A username login string is matched against the first domain style enabled. Then, if the username login string is not decoded, it is matched against the second domain style enabled.

**Examples** To enable NT domain style on the local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# domain-style ntdomain
```

To disable NT domain style on the local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no domain-style ntdomain
```

**Related commands** [server enable](#)

## egress-vlan-id (radsrv-grp)

**Overview** Use this command to configure the standard RADIUS attribute 'Egress-VLANID (56)' for the local RADIUS Server user group.

Use the **no** variant of this command to remove the Egress-VLANID attribute from the local RADIUS server user group.

**Syntax** `egress-vlan-id <vid> [tagged|untagged]`  
`no egress-vlan-id`

| Parameter | Description                                                                                                                       |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------|
| <vid>     | The VLAN identifier to be used for the Egress VLANID attribute, in the range 1 to 4094.                                           |
| tagged    | Set frames on the VLAN as tagged. This sets the tag indication field to indicate that all frames on this VLAN are tagged.         |
| untagged  | Set all frames on the VLAN as untagged. This sets the tag indication field to indicate that all frames on this VLAN are untagged. |

**Default** By default, no Egress-VLANID attributes are configured.

**Mode** Local RADIUS Server User Group Configuration

**Examples** To set the 'Egress-VLANID' attribute for the 'NormalUsers' local RADIUS server user group to VLAN identifier 200, with tagged frames, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# egress-vlan-id 200 tagged
```

To remove the 'Egress-VLANID' attribute for the 'NormalUsers' local RADIUS server user group, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no egress-vlan-id
```

**Related commands** [attribute \(radsrv-grp\)](#)  
[egress-vlan-name \(radsrv-grp\)](#)



## egress-vlan-name (radsrv-grp)

**Overview** Use this command to configure the standard RADIUS attribute 'Egress-VLAN-Name (58)' for the local RADIUS server user group.

Use the **no** variant of this command to remove the Egress-VLAN-Name attribute from the local RADIUS server user group.

**Syntax** `egress-vlan-name <vlan-name> [tagged|untagged]`  
`no egress-vlan-name`

| Parameter   | Description                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <vlan-name> | The VLAN name to be configured as the Egress-VLAN-Name attribute.                                                                 |
| tagged      | Set frames on the VLAN as tagged. This sets the tag indication field to indicate that all frames on this VLAN are tagged.         |
| untagged    | Set all frames on the VLAN as untagged. This sets the tag indication field to indicate that all frames on this VLAN are untagged. |

**Default** By default, no Egress-VLAN-Name attributes are configured.

**Mode** Local RADIUS Server User Group Configuration

**Examples** To configure the 'Egress-VLAN-Name' attribute for the RADIUS server user group 'NormalUsers' with the VLAN name vlan2 and all frames on this VLAN tagged, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# egress-vlan-name vlan2 tagged
```

To delete the 'Egress-VLAN-Name' attribute for the 'NormalUsers' group, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no egress-vlan-name
```

**Related commands** [attribute \(radsrv-grp\)](#)  
[egress-vlan-id \(radsrv-grp\)](#)

# group (radsrv)

**Overview** Use this command to create a local RADIUS server user group, and enter local RADIUS Server User Group Configuration mode.

Use the **no** variant of this command to delete the local RADIUS server user group.

**Syntax** `group <user-group-name>`  
`no group <user-group-name>`

| Parameter                            | Description             |
|--------------------------------------|-------------------------|
| <code>&lt;user-group-name&gt;</code> | User group name string. |

**Mode** RADIUS Server Configuration

**Examples** The following command creates the user group NormalUsers.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
```

The following command deletes the user group NormalUsers.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no group NormalUsers
```

**Related commands** [user \(radsrv\)](#)  
[show radius local-server user](#)  
[vlan \(radsrv-grp\)](#)

# help radius-attribute

**Overview** Use this command to display a list of standard and vendor specific valid RADIUS attributes that are supported by the local RADIUS server.

**Syntax** `help radius-attribute [<attribute-name>|<attribute-ID>]`

| Parameter                           | Description                                                        |
|-------------------------------------|--------------------------------------------------------------------|
| <code>&lt;attribute-name&gt;</code> | List the details and predefined values for the named attribute.    |
| <code>&lt;attribute-ID&gt;</code>   | List the details and predefined values for the given attribute ID. |

**Mode** Privileged Exec

**Usage notes** When used without a parameter, this command lists all of the available RADIUS attributes.

When used with an attribute name or ID, this command displays the attribute name, value type, and any predefined values.

**Example** To list all available RADIUS attributes, use the following command:

```
awplus# help radius-attribute
```

```
awplus#help radius-attribute
Standard Attributes:
 1 User-Name
 2 User-Password
 3 CHAP-Password
 4 NAS-IP-Address
 5 NAS-Port
 6 Service-Type
...
```

To display the details for the RADIUS attribute Frag-Status, use the following command:

```
awplus# help radius-attribute frag-status
```

```
awplus#help radius-attribute frag-status
Frag-Status : integer (Integer number)

Pre-defined values :
 Fragmentation-Supported (1)
 More-Data-Pending (2)
 More-Data-Request (3)
 Reserved (0)
```

**Related commands** [attribute \(radsrv-grp\)](#)

**Command changes** Version 5.4.8-0.2: command added  
Version 5.4.9-0.1: added to x530 Series products

# nas

**Overview** This command adds a client device (the Network Access Server or the NAS) to the list of devices that are able to send authentication requests to the local RADIUS server. The NAS is identified by its IP address and a shared secret (also referred to as a shared key) must be defined that the NAS will use to establish its identity.

Use the **no** variant of this command to remove a NAS client from the list of devices that are allowed to send authentication requests to the local RADIUS server.

**Syntax** `nas <ip-address> key <nas-keystring>`  
`no nas <ip-address>`

| Parameter                          | Description            |
|------------------------------------|------------------------|
| <code>&lt;ip-address&gt;</code>    | RADIUS NAS IP address. |
| <code>&lt;nas-keystring&gt;</code> | NAS shared keystring.  |

**Mode** RADIUS Server Configuration

**Examples** The following commands add the NAS with an IP address of 192.168.1.2 to the list of clients that may send authentication requests to the local RADIUS server. Note the shared key that this NAS will use to establish its identity is NAS\_PASSWORD.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# nas 192.168.1.2 key NAS_PASSWORD
```

The following commands remove the NAS with an IP address of 192.168.1.2 from the list of clients that are allowed to send authentication requests to the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no nas 192.168.1.2
```

**Related commands** [nas message-authenticator \(radsrv\)](#)  
[show radius local-server nas](#)

## nas message-authenticator (radsvr)

**Overview** Use this command to decide whether or not to require verification of RADIUS packets for a specific NAS. Verification prevents RADIUS protocol forgery attacks. It is achieved by putting a Message-Authenticator attribute in Access-Requests from the NAS.

Use the **no** variant of this command to return the setting to the default.

**Syntax** `nas <ip-address> message-authenticator  
{required|optional|auto}`  
`no nas <ip-address> message-authenticator`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-address> | The IP address of the NAS.                                                                                                                                                                                                                                                                                                                        |
| required     | Discard Access-Requests that have no Message-Authenticator attribute, or that have an invalid Message-Authenticator attribute.                                                                                                                                                                                                                    |
| optional     | Allow Access-Requests that have no Message-Authenticator attribute, and discard Access-Requests that have an invalid Message-Authenticator attribute.                                                                                                                                                                                             |
| auto         | Determine the mode based on the content of the first Access-Request received. On the basis of this, the device will produce a log message to tell you which mode you should configure. Only use <b>auto</b> temporarily while you are transitioning an existing network or adding new NAS devices with unknown support for Message-Authenticator. |

**Default** auto

**Mode** RADIUS Server Configuration

**Usage notes** If you use both MAC authentication and web authentication to authenticate the same TQ Series access point, make sure you set this to **optional**. Otherwise, web authentication may fail.

This is because if the first packet that the server receives from the client contains a valid Message-Authenticator attribute, then by default all subsequent packets from that client must also contain the same Message-Authenticator attribute. If packets don't contain the attribute, the server drops them. This can cause an issue on TQ series APs, because on these APs, MAC authentication's initial packet contains the attribute, and web authentication's initial packet doesn't. This means that web authentication will fail if MAC authentication has already happened.

Setting this to **optional** allows the server to accept packets from a client when the packets don't have a Message-Authenticator attribute, even if the server has already received a packet from that client that contained a Message-Authenticator attribute. This means both web authentication and MAC authentication will succeed, no matter which happens first.

**Examples** To require Message-Authenticator attributes in messages from a registered NAS whose IP address is 192.168.1.2, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsvr)# nas 192.168.1.2 message-authenticator
required
```

To make Message-Authenticator attributes optional in messages from a registered NAS whose IP address is 192.168.1.9, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsvr)# nas 192.168.1.9 message-authenticator
optional
```

To return to the default behavior of **auto** for the NAS whose IP address is 192.168.1.9, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsvr)# no nas 192.168.1.9 message-authenticator
```

**Related commands** [ip radius require-message-authenticator](#)  
[nas](#)  
[show radius local-server nas](#)

**Command changes** Version 5.5.4-2.3: command added

# radius-secure-proxy local-server

**Overview** Use this command to enter the RadSecProxy local-server application configuration mode. This application allows remote RadSec clients to communicate with the local RADIUS server process via a secure (TLS) proxy.

**Syntax** `radius-secure-proxy local-server`

**Mode** Global Configuration Mode

**Example** To change mode from User Exec mode to the RadSecProxy local-server configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy local-server
awplus(config-radsecproxy-srv)#
```

**Related commands**

- `client (radsecproxy-srv)`
- `client name-check`
- `client trustpoint`



# radius-server local

**Overview** Use this command to navigate to the Local RADIUS server configuration mode (`config-radsrv`) from the Global Configuration mode (`config`).

**Syntax** `radius-server local`

**Mode** Global Configuration

**Example** Local RADIUS Server commands are available from `config-radsrv` configuration mode. To change mode from User Exec mode to the Local RADIUS Server mode (`config-radsrv`), use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)#
```

## Output

```
awplus(config)#radius-server local
Creating Local CA repository.....OK
Enrolling Local System to local trustpoint..OK
awplus(config-radsrv)#
```

**Related commands**

- `server enable`
- `show radius local-server group`
- `show radius local-server nas`
- `show radius local-server statistics`
- `show radius local-server user`

# server auth-port

**Overview** Use this command to change the UDP port number for local RADIUS server authentication.

Use the **no** variant of this command to reset the RADIUS server authentication port back to the default.

**Syntax** `server auth-port <1-65535>`  
`no server auth-port`

| Parameter | Description      |
|-----------|------------------|
| <1-65535> | UDP port number. |

**Default** The default local RADIUS server UDP authentication port number is 1812.

**Mode** RADIUS Server Configuration

**Examples** The following commands set the RADIUS server authentication port to 10000.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server auth-port 10000
```

The following commands reset the RADIUS server authentication port back to the default UDP port of 1812.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no server auth-port
```

**Related commands** [server enable](#)  
[show radius local-server statistics](#)

# server enable

**Overview** This command enables the local RADIUS server. The local RADIUS server feature is started immediately when this command is issued.

The **no** variant of this command disables local RADIUS server. When this command is issued, the local RADIUS server stops operating.

**Syntax** `server enable`  
`no server enable`

**Default** The local RADIUS server is disabled by default and must be enabled for use with this command.

**Mode** RADIUS Server Configuration

**Examples** To enable the local RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server enable
```

To disable the local RADIUS server, use the command:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no server enable
```

**Related commands** [server auth-port](#)  
[show radius local-server statistics](#)

# server trustpoint (radsrv)

**Overview** Use this command to add one or more trustpoints to the local RADIUS server. You can specify multiple trustpoints on one line, or execute the command more than once to add multiple trustpoints to the local RADIUS server.

Use the **no** variant to remove one or more trustpoints from the local RADIUS server.

**Syntax** `server trustpoint [<trustpoint-list>]`  
`no server trustpoint [<trustpoint-list>]`

| Parameter         | Description                                            |
|-------------------|--------------------------------------------------------|
| <trustpoint-list> | Specify one or more trustpoints to be added or deleted |

**Default** By default, the local trustpoint is associated with the local RADIUS server.

**Mode** RADIUS Server Configuration

**Usage Notes** If you do not specify any trustpoints, the command displays a list of trustpoints but leaves the list unchanged.

If you use the **no server trustpoint** command without specifying any trustpoints, then all trustpoints will be removed from the local RADIUS server.

**Example** To configure a trustpoint called 'my\_trustpoint' on the local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server trustpoint my_trustpoint
```

You can add multiple trustpoints to the local RADIUS server by executing the **server trustpoint** command multiple times:

```
awplus(config-radsrv)# server trustpoint my_trustpoint1
my_trustpoint2
```

To remove the trustpoint called 'my\_trustpoint' from the local RADIUS server, use the command:

```
awplus(config-radsrv)# no server trustpoint my_trustpoint
```

To remove all trustpoints from the local RADIUS server, use the command:

```
awplus(config-radsrv)# no server trustpoint
```

**Related commands** [show radius local-server trustpoint](#)  
[server enable](#)  
[client trustpoint](#)  
[server trustpoint](#)

**Command changes** Version 5.4.1-1.1: command added.

# show radius local-server group

**Overview** Use this command to display information about the local RADIUS server user group.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show radius local-server group [<user-group-name>]`

| Parameter                            | Description             |
|--------------------------------------|-------------------------|
| <code>&lt;user-group-name&gt;</code> | User group name string. |

**Mode** User Exec and Privileged Exec

**Example** The following command displays Local RADIUS server user group information.

```
awplus# show radius local-server group
```

## Output

**Table 1:** Example output from the **show radius local-server group** command

|                  |               |
|------------------|---------------|
| Group-Name       | Vlan          |
| -----            |               |
| NetworkOperators | ManagementNet |
| NormalUsers      | CommonNet     |

**Table 2:** Parameters in the output of the **show radius local-server group** command

| Parameter  | Description                      |
|------------|----------------------------------|
| Group-Name | Group name.                      |
| Vlan       | VLAN name assigned to the group. |

**Related commands** [group \(radsrv\)](#)

# show radius local-server nas

**Overview** Use this command to display information about NAS (Network Access Servers) registered to the local RADIUS server.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show radius local-server nas [<ip-address>]`

| Parameter    | Description                             |
|--------------|-----------------------------------------|
| <ip-address> | Specify NAS IP address for show output. |

**Mode** User Exec and Privileged Exec

**Example** The following command displays NAS information.

```
awplus# show radius local-server nas
```

## Output

**Table 3:** Example output from the **show radius local-server nas** command

| NAS-Address | Shared-Key (encrypted) | Message Authenticator |
|-------------|------------------------|-----------------------|
| 127.0.0.1   | dbSQ8ED....            | optional              |

**Table 4:** Parameters in the output of the **show radius local-server nas** command

| Parameter             | Description                            |
|-----------------------|----------------------------------------|
| NAS-Address           | IP address of NAS.                     |
| Shared-Key            | Shared key used for RADIUS connection. |
| Message Authenticator | The message-authenticator mode.        |

**Related commands** [nas](#)  
[nas message-authenticator \(radsvr\)](#)

# show radius local-server statistics

**Overview** Use this command to display statistics about the local RADIUS server.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show radius local-server statistics`

**Mode** User Exec and Privileged Exec

**Usage notes** Both unknown usernames and invalid passwords will display as failed logins in the show output.

**Example** The following command displays local RADIUS server statistics.

```
awplus# show radius local-server statistics
```

## Output

**Table 5:** Example output from the **show radius local-server statistics** command

|                                             |   |                                       |                           |
|---------------------------------------------|---|---------------------------------------|---------------------------|
| awplus# show radius local-server statistics |   |                                       |                           |
| Server status                               | : | Run (administrative status is enable) |                           |
| Enabled methods                             | : | MAC EAP-MD5 EAP-TLS EAP-PEAP          |                           |
| Available methods                           | : | MAC EAP-MD5 EAP-TLS EAP-PEAP          |                           |
| EAP trustpoints                             | : | local                                 |                           |
| Promiscuous mode                            | : | Enabled                               |                           |
| Successes                                   | : | 7                                     | Unknown NAS :0            |
| Failed Logins                               | : | 0                                     | Invalid packet from NAS:0 |
| Internal Error                              | : | 0                                     | Unknown Error :0          |
| NAS : 127.0.0.1                             |   |                                       |                           |
| Successes                                   | : | 7                                     | Shared key mismatch :0    |
| Failed Logins                               | : | 0                                     | Unknown RADIUS message :0 |
| Unknown EAP message                         | : | 0                                     | Unknown EAP auth type :0  |
| Corrupted packet                            | : | 0                                     |                           |
| Users present in the User Database:         |   |                                       |                           |
| Username                                    |   | Successes                             | Failures LastInteraction  |
|                                             |   |                                       | Local time (+00:00)       |



**Table 5:** Example output from the **show radius local-server statistics** command (cont.)

|                                         |           |          |                      |
|-----------------------------------------|-----------|----------|----------------------|
| 00-00-00-00-00-01                       | 0         | 0        | -                    |
| 00-00-00-00-00-02                       | 0         | 0        | -                    |
| 00-15-65-3f-d9-42                       | 0         | 0        | -                    |
| 00-90-0b-45-07-e4                       | 4         | 0        | 09 Jan               |
| 2024 00:32:24                           |           |          |                      |
| tester1                                 | 2         | 0        | 09 Jan               |
| 2024 00:31:52                           |           |          |                      |
| tester2                                 | 0         | 0        | -                    |
| user1                                   | 0         | 0        | -                    |
| user1dynvlan                            | 0         | 0        | -                    |
| user2dynvlan                            | 0         | 0        | -                    |
| Users NOT present in the User Database: |           |          |                      |
| Username                                | Successes | Failures | Last Interaction     |
|                                         |           |          | Local time (+00:00)  |
| 00-90-0b-45-07-e2                       | 1         | 0        | 09 Jan 2024 00:31:50 |

- Related commands

clear radius local-server statistics

radius-server local

server enable

server auth-port

# show radius local-server trustpoint

**Overview** Displays the PKI trustpoints associated with the local RADIUS server.

**Syntax** `show radius local-server trustpoint`

**Mode** User Exec

**Example** To show the local RADIUS server trustpoint(s), use the commands:

```
show radius local-server trustpoint
```

**Output** Figure 37-1: Example output from **show radius local-server trustpoint**

```
show radius local-server trustpoint
Current PKI trustpoints for RADIUS EAP-TLS:
 my_trustpoint
```

**Related commands**

- [server trustpoint \(radsrv\)](#)
- [radius-server local](#)
- [server enable](#)
- [show radius local-server statistics](#)

**Command changes** Version 5.4.6-1.1: command added

# show radius local-server user

**Overview** Use this command to display information about the local RADIUS server user.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax**

```
show radius local-server user [<user-name>]
show radius local-server user [<user-name>] format csv
show radius local-server user [<user-name>] detail
```

| Parameter   | Description                                                                             |
|-------------|-----------------------------------------------------------------------------------------|
| <user-name> | RADIUS user name. If no user name is specified, information for all users is displayed. |
| format csv  | Format output as CSV. This parameter is only available in Privileged Exec mode.         |
| detail      | Display detailed information about the user.                                            |

**Mode** User Exec and Privileged Exec

**Examples** The following command displays Local RADIUS server user information for user Tom.

```
awplus# show radius local-server user Tom
```

**Table 6:** Example output from the **show radius local-server user** command

| User-Name | Group            | Vlan          |
|-----------|------------------|---------------|
| Tom       | NetworkOperators | ManagementNet |

The following command displays all Local RADIUS server information for all users.

```
awplus# show radius local-server user
```

The following command displays Local RADIUS server user information for Tom in CSV format (only available in Privileged Exec mode).

```
awplus# show radius local-server user Tom format csv
```

**Table 7:** Example output from the **show radius local-server user Tom format csv** command

|                                                                                                                                                         |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| true,"NetworkOperators","Tom","abcd",0,2099/01/01,1,"",,"ManagementNet"false,3600,false,0,"",false,"",false,false,"",,"",false,false,,false,0,0,"",true |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|

The following command displays detailed Local RADIUS server user information for all users.

```
awplus# show radius local-server user detail
```

**Table 8:** Example output from the **show radius local-server user detail** command

```
awplus# show radius local-server user detail
Total users: 1
Maximum users allowed by license: 3

Username : Tom
Group : NetworkOperators
Vlan : VlanName
```

**Table 9:** Parameters in the output from the **show radius local-server user** command

| Parameter | Description                      |
|-----------|----------------------------------|
| User-Name | User name.                       |
| Group     | Group name assigned to the user. |
| Vlan      | VLAN name assigned to the user.  |

**Related commands**    [group \(radsrv\)](#)  
                      [user \(radsrv\)](#)

**Command changes**    Version 5.4.9-0.1: **detail** parameter added

## user (radsrv)

**Overview** Use this command to register a user to the local RADIUS server.

Use the **no** variant of this command to delete a user from the local RADIUS server.

**Syntax** `user <radius-user-name> [encrypted] password <user-password>  
[group <user-group>]`

`no user <radius-user-name>`

| Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <radius-user-name> | RADIUS user name. This can also be a MAC address in the IEEE standard format of HH-HH-HH-HH-HH-HH if you are configuring MAC authentication to use local RADIUS server.                                                                                                                                                                                                                                                                                                                                                                           |
| encrypted          | Specifies that the password is being entered in its encrypted form, so that it is not further encrypted. When creating a new user, enter the password in plaintext, and do not use the <b>encrypted</b> parameter. Use the <b>encrypted</b> parameter only when referring to a user that has previously been created. For instance, when adding an existing user from another RADIUS server, use the <b>encrypted</b> parameter, and enter the encrypted version of the password that appears in the output of <b>show</b> commands for the user. |
| <user-password>    | User password. This can also be a MAC address in the IEEE standard format of HH-HH-HH-HH-HH-HH if you are configuring MAC authentication to use local RADIUS server.                                                                                                                                                                                                                                                                                                                                                                              |
| group              | Specify the group for the user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <user-group>       | User group name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

**Mode** RADIUS Server Configuration

**Usage notes** RADIUS user names cannot contain question mark (?), space ( ), or quote (" ") characters. RADIUS user names containing the below characters cannot use certificate authentication:

/ \ '\$ & ( ) \* ; < > ` |

Certificates cannot be created and exported for RADIUS user names that contain the above characters. We advise you to avoid using these characters in RADIUS user names if you need to use certificate authentication, because you will not be able to create and export certificates.

You also can use the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) to specify a supplicant MAC address to configure the user name and user password parameters to use local RADIUS server for MAC Authentication. See the [AAA and Port\\_Authentication Feature Overview and Configuration\\_Guide](#) for a sample MAC configuration. See also the command **user**

**00-db-59-ab-70-37 password 00-db-59-ab-70-37** as shown in the command examples.

**Examples** The following commands add user 'Tom' to the local RADIUS server and sets his password to 'QwerSD'.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user Tom password QwerSD
```

The following commands add user 'Tom' to the local RADIUS server user group 'NormalUsers' and sets his password 'QwerSD'.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user Tom password QwerSD group
NormalUsers
```

The following commands remove user 'Tom' from the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no user Tom
```

The following commands add the supplicant MAC address 00-d0-59-ab-70-37 to the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user 00-db-59-ab-70-37 password
00-db-59-ab-70-37
```

The following commands remove the supplicant MAC address 00-d0-59-ab-70-37 from the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no user 00-db-59-ab-70-37
```

**Related commands** [group \(radsrv\)](#)  
[show radius local-server user](#)

## vlan (radsrv-grp)

**Overview** Use this command to set the VLAN ID or name for the local RADIUS server user group. The VLAN information is used for authentication with the dynamic VLAN feature.

Use the **no** variant of this command to clear the VLAN ID or VLAN name for the local RADIUS server user group.

**Syntax** `vlan {<vid>|<vlan-name>}`  
`no vlan`

| Parameter                      | Description |
|--------------------------------|-------------|
| <code>&lt;vid&gt;</code>       | VLAN ID.    |
| <code>&lt;vlan-name&gt;</code> | VLAN name.  |

**Default** VLAN information is not set by default.

**Mode** Local RADIUS Server User Group Configuration

**Examples** The following commands set VLAN ID 200 to the group named 'NormalUsers':

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# vlan 200
```

The following commands remove VLAN ID 200 from the group named 'NormalUsers':

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no vlan
```

**Related commands** [group \(radsrv\)](#)  
[show radius local-server user](#)

# 38

# Two-factor Authentication (2FA) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure two-factor authentication (2FA).

2FA is a method of strengthening security by requiring a second method of authentication. AlliedWare Plus supports 2FA on OpenVPN connections. It requires a software-based authenticator that implements either the time-based one-time password (TOTP) or the HMAC-based one-time password (HOTP) algorithms. These software authenticators (known as authenticator apps) are usually loaded on a mobile device. One well-known implementation of such an app is Google Authenticator.

For more information on configuring 2FA on OpenVPN, see the “Two-factor authentication” chapter in the [OpenVPN Feature Overview and Configuration Guide](#).

- Command List**
- “[2fa allow-reuse](#)” on page 1734
  - “[2fa create user](#)” on page 1735
  - “[2fa create user email](#)” on page 1737
  - “[2fa create user skip-2fa](#)” on page 1738
  - “[2fa delete user](#)” on page 1739
  - “[2fa email-expiry-time](#)” on page 1740
  - “[2fa email-otp](#)” on page 1741
  - “[2fa email-template](#)” on page 1742
  - “[2fa export user-data](#)” on page 1744
  - “[2fa hotp-window-size](#)” on page 1745
  - “[2fa import user-data source](#)” on page 1746
  - “[2fa issuer](#)” on page 1748
  - “[2fa label](#)” on page 1750



- ["2fa max-skew"](#) on page 1752
- ["2fa radius-email-attribute"](#) on page 1753
- ["2fa reject-unconfigured-users"](#) on page 1755
- ["2fa reset scratch-codes"](#) on page 1756
- ["2fa reset skew"](#) on page 1757
- ["2fa skew adjust"](#) on page 1758
- ["2fa totp-window-size"](#) on page 1760
- ["2fa self-registration port"](#) on page 1761
- ["aaa authentication 2fa-registration default group"](#) on page 1763
- ["debug 2fa"](#) on page 1765
- ["email-attribute \(ldap-server\)"](#) on page 1766
- ["service 2fa"](#) on page 1767
- ["show 2fa"](#) on page 1769
- ["show 2fa email-template"](#) on page 1770
- ["show 2fa user"](#) on page 1771
- ["show 2fa users"](#) on page 1773
- ["show debugging 2fa"](#) on page 1774
- ["undebg 2fa"](#) on page 1775

# 2fa allow-reuse

**Overview** Use this command, when configuring two-factor authentication (2FA), to allow the reuse of time-based codes within the acceptable time window. By default, if a code has already been used then it will be rejected. This means the user must wait for the next code to appear in their authenticator app to be able to login.

Use the **no** variant of this command to return to the default state, which is to reject codes that have already been used.

**Syntax** `2fa allow-reuse`  
`no 2fa allow-reuse`

**Default** Disabled

**Mode** Global Configuration

**Usage notes** The 2FA service must be running for this command to work. Enable it with the [service 2fa](#) command.

**Example** To allow the reuse of time-based codes, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa allow-reuse
```

To prevent the reuse of time-based codes, use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa allow-reuse
```

**Related commands** [2fa create user](#)  
[2fa delete user](#)  
[service 2fa](#)  
[show 2fa](#)  
[show 2fa user](#)  
[show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added

## 2fa create user

**Overview** Use this command to create the two-factor authentication (2FA) data for a user. It allows you to set the authentication mode, HMAC-based One-Time Password (HOTP) or Time-based one-time password (TOTP), and displays a QR code and scratch codes for the user.

For more information on configuring 2FA on OpenVPN, see the “Two-factor authentication” chapter in the [OpenVPN Feature Overview and Configuration Guide](#).

**Syntax** `2fa create user <user-name> {random-secret|secret <secret-key>} [hotp] [qr {ansi|utf8|link}]`

| Parameter     | Description                                                                                                                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <user-name>   | The name of the user you are creating.                                                                                                                                                                                      |
| random-secret | Generate a random secret key.                                                                                                                                                                                               |
| secret        | Use a pre-defined secret key.                                                                                                                                                                                               |
| <secret-key>  | The pre-defined secret key.                                                                                                                                                                                                 |
| hotp          | Use HOTP mode for code verification (the default is TOTP).                                                                                                                                                                  |
| qr            | Display the QR code                                                                                                                                                                                                         |
| ansi          | Display the QR code using ANSI block characters.                                                                                                                                                                            |
| utf8          | Display the QR code using a UTF-8 mosaic.                                                                                                                                                                                   |
| link          | Display a hyperlink for a QR code generator. Opening the link in a browser will display a QR code. As the string is passed to an online QR code generator (at Google), it may be a security concern for some installations. |

**Mode** Privileged Exec

**Usage notes** You must enable the 2FA service, with the [service 2fa](#) command, before creating user data.

The QR code displays best in a color mode ANSI or UTF-8 terminal. If your terminal is insufficiently wide, or doesn't have the correct options enabled, you may not get a scannable QR code.

**Example** To create a user ‘test’, generate a random secret key, use HOTP mode, and display a QR link, use the command:

```
awplus# 2fa create user test random-secret hotp qr link
```

**Output** Figure 38-1: Example output from **2fa create user test random-secret hotp qr link**

```
awplus#2fa create user test random-secret hotp qr link
Two-Factor Authentication information for user:

Username: test
Secret: IWNZKQS2WXQ6I2VHGTUFP4IVA4
Mode: HOTP (counter: 1)
OTP URL:otppath://hotp/test@awplus?secret=IWNZKQS2WXQ6I2VHGTUFP4IVA4
Scratch codes:
59808697
25389232
71366922
48035778
82664010

The following URL can be used to generate a QR code.
This results in the user key being sent to Google servers.
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otppath://hotp/test@awplus%3Fsecret%3DIWNZKQS2WXQ6I2VHGTUFP4IVA4awplus#
```

**Related commands**

- [2fa delete user](#)
- [2fa reset skew](#)
- [2fa reset scratch-codes](#)
- [service 2fa](#)
- [show 2fa](#)
- [show 2fa user](#)
- [show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added

## 2fa create user email

**Overview** Use this command to create a Two-Factor Authentication (2FA) email user entry. This allows users authenticating through OpenVPN to use the 2FA email One-Time-Password feature (2FA email OTP).

**Syntax** `2fa create user <user-name> email <email-address>`

| Parameter                          | Description                                      |
|------------------------------------|--------------------------------------------------|
| <code>&lt;user-name&gt;</code>     | User name, for example, 'test1'                  |
| <code>&lt;email-address&gt;</code> | User email address, for example, 'test1@xyz.com' |

**Default** No user email is created.

**Mode** Privileged Exec

**Usage notes** 2FA users can be emailed their OTP instead of using their mobile device app to generate their OTP.

**Example** To configure the user 'test1' with the email address 'test1@xyz.com', use the command:

```
awplus# c2fa create user test1 email test1@xyz.com
```

**Related commands**

- [2fa create user](#)
- [2fa delete user](#)
- [service 2fa](#)
- [2fa create user skip-2fa](#)

**Command changes** Version 5.5.3-0.1: command added

## 2fa create user skip-2fa

**Overview** Use this command to create a Two-Factor Authentication skip-2fa user entry. This enables users authenticating through OpenVPN to skip 2FA requirements.

This means that these users do not need to generate One-Time-Passwords (OTP) from a time-based OTP authenticator app or email OTP code.

**Syntax** `2fa create user <user-name> skip-2fa`

| Parameter                      | Description                                |
|--------------------------------|--------------------------------------------|
| <code>&lt;user-name&gt;</code> | The name of the user, for example, 'Test1' |

**Default** No 2FA skip-2fa user entry exists.

**Mode** Privileged Exec

**Usage notes** To remove a 2FA skip-2fa user entry, use the command **2fa delete user**.

**Example** To create a user named 'Test1' that can skip the 2FA requirements, use the command:

```
awplus# 2fa create user Test1 skip-2fa
```

**Related commands** [2fa create user](#)  
[2fa delete user](#)  
[2fa create user email](#)

**Command changes** Version 5.5.3-0.1: command added

# 2fa delete user

**Overview** Use this command to delete the two-factor authentication (2FA) data for a user.

**Syntax** `2fa delete user <user-name>`

| Parameter                      | Description                            |
|--------------------------------|----------------------------------------|
| <code>&lt;user-name&gt;</code> | The name of the user you are deleting. |

**Mode** Privileged Exec

**Example** To delete the 2FA data for a user named 'test', use the command:

```
awplus# 2fa delete user test
```

**Related commands**

- [2fa create user](#)
- [2fa reset scratch-codes](#)
- [2fa reset skew](#)
- [service 2fa](#)
- [show 2fa user](#)
- [show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added

# 2fa email-expiry-time

**Overview** A Two-Factor Authentication (2FA) user email code will be valid only for a certain time after it is generated. The default time period is 10 minutes. This command sets an expiry time globally.

Use the **no** variant of this command to reset the expiry time back to the default (10 minutes).

**Syntax** `2fa email-expiry-time <1-1440>`  
`no 2fa email-expiry-time`

| Parameter                   | Description                                          |
|-----------------------------|------------------------------------------------------|
| <code>&lt;1-1440&gt;</code> | The expiry time in minutes, for example, 20 minutes. |

**Default** 10 minutes

**Mode** Global Configuration

**Examples** To set 2FA user email OTP expiry time to 20 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa email-expiry-time 20
```

To reset 2FA user email OTP expiry time back to the default (10 minutes), use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa email-expiry-time
```

**Related commands** [2fa email-otp](#)  
[2fa email-template](#)  
[service 2fa](#)

**Command changes** Version 5.5.3-01: command added



## 2fa email-otp

**Overview** Use this command to enable the Two-Factor Authentication email One-Time-Password (OTP) feature. The 2FA email OTP feature emails the password instead of receiving it with an authenticating mobile app. The emailed OTP allows you to connect to an OpenVPN tunnel.

Use the **no** variant of this command to disable the 2FA email OTP feature.

**Syntax** `2fa email-otp`  
`no 2fa email-otp`

**Default** Disabled

**Mode** Global Configuration

**Examples** To enable the 2FA email OTP feature, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa email-otp
```

To disable the 2FA email OTP feature, use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa email-otp
```

**Output** Figure 38-2: Example output from **2fa email-otp**

```
Sub-feature 2FA email OTP is enabled
```

**Related commands** [service 2fa](#)

**Command changes** Version 5.5.3-0.1: command added

## 2fa email-template

**Overview** Use this command to set the location of the Two-Factor Authentication email One-Time-Password (2FA email OTP) template file.

Use the **no** variant of this command to set the email template file back to the default.

**Syntax** `2fa email-template <file-name>`  
`no 2fa email-template`

| Parameter                      | Description                                                                                                 |
|--------------------------------|-------------------------------------------------------------------------------------------------------------|
| <code>&lt;file-name&gt;</code> | The name of the email template file saved to flash memory on your device, for example 'email_template.txt'. |

**Default** Figure 38-3: Default email template file contents

```
Subject: %%LABEL%% 2FA Email OTP code

Verification code: %%OTP%%

The verification code will expire in %%EXPIRY_TIME%% minutes.
This is an automated message, please do not reply.
```

**Mode** Global Configuration

**Usage notes** A subject line with an empty line immediately following it is required. There are some words surrounded by %% signs. These are replaced by the specified details when the email is sent. There are five different options for these, each of which can be used multiple times if needed:

Table 38-1: Parameter options for the email template

| Template Parameter | Description                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------|
| %%OTP%%            | The OTP code that the user can use to log in. This must be included in the template.                         |
| %%USERNAME%%       | The username of the user who is attempting to connect.                                                       |
| %%EMAIL_ADDR%%     | The email address of the user, which the email will be sent to.                                              |
| %%EXPIRY_TIME%%    | The number of minutes that the OTP will be valid for.                                                        |
| %%LABEL%%          | A configurable label that is set by the 2FA configuration, which is also displayed in application-based 2FA. |

**Example** To configure an email template, first the new email template needs to be saved to a file on the flash memory of your device. For example:

Figure 38-4: Example email template file named **email\_template.txt**

```
Subject: %%LABEL%% 2FA Email OTP code for %%USERNAME%%

Verification code: %%OTP%%

The verification code will expire in %%EXPIRY_TIME%% minutes.
This is an automated message, please do not reply.

This email was intended for %%EMAIL_ADDRESS%%.
Send by %%LABEL%%
```

To configure the template file named 'email\_template.txt', use the commands:

```
awplus# configure terminal
awplus(config)# 2fa email-template email_template.txt
```

**Related  
commands**

[2fa label](#)  
[2fa email-otp](#)  
[2fa email-expiry-time](#)  
[show 2fa email-template](#)

**Command  
changes**

Version 5.5.3-0.1: command added

## 2fa export user-data

**Overview** Use this command to export Two-Factor Authentication (2FA) user data to a flash file.

**Syntax** `2fa export user-data`

**Default** No files are exported

**Mode** Privileged Exec

**Usage notes** 2FA user data will be exported to a local flash file only. The data will be compressed and encrypted with a password. An administrator transports the flash file and copies it to a location where it can then be copied to another AlliedWare plus device for importation.

Use the command **2fa import user-data source** to import the user data after exporting it with this command.

**Example** To export 2FA user data to a flash file, use the command:

```
awplus# 2fa export user-data
```

**Output** Figure 38-5: Example output from **2fa export user-data**

```
awplus#2fa export user-data
Enter security password:
Re-enter password:
Successfully exported 2FA user data (11 users) to file
atl2fausers-20230303-3272.dat
awplus#
```

**Related commands** [2fa import user-data source](#)

**Command changes** Version 5.5.3-0.1: command added

## 2fa hotp-window-size

**Overview** Use this command to set the range of acceptable codes for HMAC-based one-time password (HOTP) mode two-factor authentication (2FA). The window size is the number of codes checked, starting at the current stored counter value, and then checking forward.

Use the **no** variant of this command to reset the window size to the default of 3.

**Syntax** `2fa hotp-window-size <1-100>`  
`no 2fa hotp-window-size`

| Parameter                  | Description                                               |
|----------------------------|-----------------------------------------------------------|
| <code>&lt;1-100&gt;</code> | The number of codes valid from the current counter value. |

**Default** 3

**Mode** Global Configuration

**Usage notes** The stored counter value is the counter value after the last successfully verified code. If a code later in the window is detected, the stored counter is updated to that value. This helps keep the mobile authenticator app and device synchronized. For example, the default HOTP window size of 3 allows the device to accept the current code or the following 2 codes.

**Example** To set the window size to include codes for the current and next 4 counter values (a total of 5 codes), use the commands:

```
awplus# configure terminal
awplus(config)# 2fa hotp-window-size 5
```

To set the window size to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa hotp-window-size
```

**Related commands**

- [2fa create user](#)
- [2fa delete user](#)
- [2fa totp-window-size](#)
- [service 2fa](#)
- [show 2fa](#)
- [show 2fa user](#)
- [show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added

## 2fa import user-data source

**Overview** Use this command to import Two-Factor Authentication (2FA) user data when you want to load the data to a different AlliedWare Plus device.

**Syntax** `2fa import user-data source <file-location> [replace]`

| Parameter                          | Description                                     |
|------------------------------------|-------------------------------------------------|
| <code>&lt;file-location&gt;</code> | The file location containing the user data.     |
| <code>replace</code>               | Indicate whether to replace existing user data. |

**Default** No user file is imported

**Mode** Privileged Exec

**Usage notes** To import user data, the 2FA service must be stopped. Use the **no** variant of the command [service 2fa](#).

Currently, the user information is stored in `flash:/configs/.atl_2fa_users`. If this file is copied to a new device before the 2FA service is started, the 2FA service will load the users at startup. This file is backed up and restored with AMF backup.

An administrator can use this command to transport the flash file and copy it to a safe location. This file can then be imported to another AlliedWare Plus device. The user data will be decompressed and decrypted with the same user password that it was exported with.

The imported user data can either replace or merge with existing 2FA user data.

**Example** In this example, the user data file is merged with any existing user data.

To import the user data file `tftp://192.168.1.1/atl2fausers-20230303-3321.dat`, use the commands:

```
awplus# c2fa import user-data source
tftp://192.168.1.1/atl2fausers-20340303-3321.dat
awplus(config)# command name
```

**Output** Figure 38-6: Example output from **2fa import user-data source**

```
awplus#2fa import user-data source
tftp://192.168.1.1/atl2fausers-20230303-3321.dat
Copying...
Successful operation
Enter security password:
Successfully imported 2FA user data (11 users).
awplus#
```

**Related commands** [2fa export user-data](#)

## service 2fa

**Command changes** Version 5.5.3-0.1: command added

## 2fa issuer

**Overview** Use this command to set an optional issuer string that is used in the two-factor authentication (2FA) QR code. The issuer string will then be set in every user's QR code.

By default, the issuer string is not set.

Use the **no** variant of this command to set the issuer string to be empty.

**Syntax** `2fa issuer <issuer-name>`  
`no 2fa issuer`

| Parameter                        | Description                                                |
|----------------------------------|------------------------------------------------------------|
| <code>&lt;issuer-name&gt;</code> | Text string to include in the OTP URL in the issuer field. |

**Default** Issuer not set

**Mode** Global Configuration

**Usage notes** The Quick Response (QR) code is built from the OTP URL. The QR code can be used to load the shared secret into an authenticator app. The label and issuer strings affect how the entry is displayed in the authenticator app.

For example, in the URL below the issuer has been set to 'ATL':

```
OTP URL: otpauth://totp/test@awplus?secret=RIVS3...&issuer=ATL
```

Once the issuer has been changed it is possible to display a QR code for existing users, with the new issuer included, by using the [show 2fa user](#) command.

The 2FA service must be running for this command to work.

**Example** To set the issuer to 'ATL', use the commands:

```
awplus# configure terminal
awplus(config)# 2fa issuer ATL
```

**Related commands**

[2fa create user](#)

[2fa delete user](#)

[2fa label](#)

[service 2fa](#)

[show 2fa](#)

[show 2fa user](#)

[show 2fa users](#)



**Command changes** Version 5.5.2-1.1: command added

## 2fa label

**Overview** Use this command to set an optional label string that is used in the two-factor authentication (2FA) QR code. The label string will be set in every user's QR code.

By default the label is the system's host name.

Use the **no** variant of this command to set the label field back to the host name.

**Syntax** `2fa label <label-string>`  
`no 2fa label`

| Parameter                         | Description                                               |
|-----------------------------------|-----------------------------------------------------------|
| <code>&lt;label-string&gt;</code> | Text string to include in the OTP URL in the label field. |

**Default** System's host name

**Mode** Global Configuration

**Usage notes** The Quick Response (QR) code is built from the OTP URL. The QR code can be used to load the shared secret into an authenticator app. The label and issuer strings affect how the entry is displayed in the authenticator app.

The full label that AlliedWare Plus produces is `<username>@<label>`. For example, in the URL below the default host name is being used with user name 'test':

```
OTP URL: otpauth://totp/test@awplus?secret=RIVS3...&issuer=ATL
```

Once the label has been changed it is possible to display a QR code for existing users, with the new label included, by using the [show 2fa user](#) command.

The 2FA service must be running for this command to work.

**Example** To set the label to 'Company VPN', use the commands:

```
awplus# configure terminal
awplus(config)# 2fa label Company VPN
```

**Related commands**

[2fa create user](#)

[2fa delete user](#)

[2fa issuer](#)

[service 2fa](#)

[show 2fa](#)

[show 2fa user](#)

[show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added

## 2fa max-skew

**Overview** Use this command to set the maximum time skew to be used by the time skew adjustment feature. The time skew adjustment feature is enabled with the [2fa skew adjust](#) command.

By default, 1500 extra codes are checked in each direction from the current time-step. This is 12.5 hours maximum skew in either direction (codes are generated in 30 second time-step intervals).

Use the **no** variant of this command to reset the maximum number of time-steps to check to 1500.

**Syntax** `2fa max-skew <120-3000>`  
`no 2fa max-skew`

| Parameter                     | Description                                      |
|-------------------------------|--------------------------------------------------|
| <code>&lt;120-3000&gt;</code> | Maximum number of 30 second time-steps to check. |

**Default** 1500

**Mode** Global Configuration

**Example** To configure the time skew adjustment feature to check a maximum of one hour (i.e. 120 30 second time-steps), either side of the current time-step, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa max-skew 120
```

To configure the time skew adjustment feature to check a maximum of 25 hours (i.e. 3000 30 second time-steps), either side of the current time-step, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa max-skew 3000
```

**Related commands** [2fa reset skew](#)  
[2fa skew adjust](#)  
[service 2fa](#)  
[show 2fa](#)  
[show 2fa user](#)  
[show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added

## 2fa radius-email-attribute

**Overview** Use this command to set the RADIUS attributes to transfer the user email address or domain to the server for Two-Factor Authentication.

These attributes are used for 2FA email One-Time-Password (OTP) to send the password to the user.

Use the **no** variant of this command to remove the RADIUS attributes from the server.

**Syntax** `2fa radius-email-attribute {email <email-address>|domain <domain-name>}`  
`no 2fa radius-email-attribute`

| Parameter       | Description                             |
|-----------------|-----------------------------------------|
| <email-address> | Email address, for example, 'User-Name' |
| <domain-name>   | Domain name, for example, 'Framed-Pool' |

**Default** No RADIUS attribute is set for user email address or domain.

**Mode** Global Configuration

**Usage notes** The RADIUS attribute for the email or domain must be an ASCII text string attribute. This can be checked by using the **help** command in AlliedWare Plus to check whether the type of an attribute is a string.

The RADIUS server can either be retrieved completely from a RADIUS attribute, or constructed using the user's username combined with the value of a RADIUS attribute containing a domain name. For example, <username>@<domain-name>.

Figure 38-7: Example output from the **help** command

```
awplus#help radius-attribute
Standard Attributes:
 1 User-Name
 2 User-Password
 3 CHAP-Password
 4 NAS-IP-Address
...
awplus#help radius-attribute framed-pool
Framed-Pool : string (Character string)
```

**Examples** To use the RADIUS attribute 'User-Name' to transfer a user's email address to the server, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa radius-email-attribute email User-Name
```

To use the RADIUS attribute 'Framed-Pool' to transfer a user's domain to the server, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa radius-email-attribute domain Framed-Pool
```

To reset the RADIUS attribute back to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa radius-email-attribute
```

**Output** Figure 38-8: Example output from **2fa radius-email-attribute**

The selected Radius attributes will be used to convey user email address or domain.

**Related commands** [2fa email-otp](#)  
[email-attribute \(ldap-server\)](#)

**Command changes** Version 5.5.3-0.1: command added

## 2fa reject-unconfigured-users

**Overview** Use this command to deny authentication to users who have not been configured for two-factor authentication (2FA). By default, if a user is not configured for 2FA then 2FA will be skipped during the authentication process.

Use the **no** variant of this command to allow users to authenticate even if they are not configured for 2FA.

**Syntax** `2fa reject-unconfigured-users`  
`no 2fa reject-unconfigured-users`

**Default** Users not configured for 2FA are allowed to authenticate.

**Mode** Global Configuration

**Example** To deny authentication to users who don't have 2FA configured, use the commands:

```
awplus# configure terminal
awplus(config)# 2fa reject-unconfigured-users
```

**Related commands**

- [2fa create user](#)
- [2fa delete user](#)
- [service 2fa](#)
- [show 2fa](#)
- [show 2fa user](#)
- [show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added

## 2fa reset scratch-codes

**Overview** Use this command to generate a set of five new scratch codes for a two-factor authentication (2FA) user. Each scratch code can only be used once.

**Syntax** `2fa reset scratch-codes user <user-name>`

| Parameter                      | Description                                              |
|--------------------------------|----------------------------------------------------------|
| <code>user</code>              | Reset scratch codes for a user.                          |
| <code>&lt;user-name&gt;</code> | Name of the user you want to generate scratch codes for. |

**Mode** Privileged Exec

**Usage notes** When a 2FA user is created, 5 scratch codes are created for that user. These are one time emergency codes that can be used in place of a code generated by the authenticator app. Once they are used, they can not be used again. Use this command to generate 5 new scratch codes for a user.

**Example** To reset the 2FA scratch codes for the user named 'test', use the command:

```
awplus# 2fa reset scratch-codes user test
```

**Output** Figure 38-9: Example output from **2fa reset scratch-codes user test**

```
Scratch codes:
 70344616
 91312817
 39931705
 89513481
 78647666
```

**Related commands**

[2fa create user](#)

[2fa delete user](#)

[2fa reset skew](#)

[show 2fa user](#)

[show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added



## 2fa reset skew

**Overview** Use this command to reset the skew adjustment data for a two-factor authentication (2FA) user. Time skew adjustment data is recorded for a user if the time skew adjustment feature is enabled with the [2fa skew adjust](#) command.

**Syntax** `2fa reset skew user <user-name>`

| Parameter   | Description                             |
|-------------|-----------------------------------------|
| user        | Reset for a user.                       |
| <user-name> | The name of the user you want to reset. |

**Mode** Privileged Exec

**Example** To reset the skew data for a user called 'test', use the command:

```
awplus# 2fa reset skew user test
```

**Related commands**

- [2fa max-skew](#)
- [2fa skew adjust](#)
- [service 2fa](#)
- [show 2fa](#)
- [show 2fa user](#)
- [show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added

## 2fa skew adjust

**Overview** Use this command to enable the time skew adjustment feature for time-based one-time password (TOTP) two-factor authentication (2FA).

TOTP authentication depends on the clock on the authenticating device and the clock on the authenticator app being synchronized. If there is a difference in time larger than what is covered by the TOTP window size then the client will not be able to authenticate. Time skew adjustment provides a method to detect and store this time difference and allow them to authenticate if it is consistent.

Use the **no** variant of this command to disable the time skew adjustment feature.

**Syntax** `2fa skew-adjust`  
`no 2fa skew-adjust`

**Default** Time skew adjustment is disabled.

**Mode** Global Configuration

**Usage notes** The most likely cause of time skew (other than the clock being set wrong on the authenticator or authenticating device) is an incorrectly configured timezone.

When time skew adjustment is enabled, extra checking happens after an incorrect login. When an incorrect login occurs, the device will check a large number of codes either side of the current time. If it finds one that matches, it will record the **skew** of the code.

If the user enters 3 incorrect (but different) codes the device checks:

- were these codes entered in quick succession, i.e. with no more than one time-step gap between them, and
- did they all have the same skew value?

If these conditions are satisfied then the device will record this as an offset (time skew) and automatically adjust which codes it checks for that user in future.

The maximum number of codes to check is configurable with the [2fa max-skew](#) command. It defaults to 12.5 hours in either direction.

If a time skew value has been stored for a user this will be displayed (with a warning) in the [show 2fa user](#) command output.

**Example** To enable the time skew adjustment feature, use the following commands:

```
awplus# configure terminal
awplus(config)# 2fa skew-adjust
```

**Related commands** [2fa max-skew](#)  
[2fa reset skew](#)  
[service 2fa](#)  
[show 2fa](#)

`show 2fa user`

`show 2fa users`

**Command changes** Version 5.5.2-1.1: command added

# 2fa totp-window-size

**Overview** Use this command to set the range of acceptable codes for time-based one-time password (TOTP) mode two-factor authentication (2FA). The window size is the number of codes checked, centered on the current time-step.

Use the **no** variant of this command to reset the window size to the default of 3.

**Syntax** `2fa totp-window-size <1-100>`  
`no 2fa totp-window-size`

| Parameter                  | Description                                                                         |
|----------------------------|-------------------------------------------------------------------------------------|
| <code>&lt;1-100&gt;</code> | The number of codes valid for a given time-step, centered on the current time-step. |

**Default** 3

**Mode** Global Configuration

**Usage notes** By default the TOTP window size is set to 3. This means that the code for the current, previous, and next 30 second time-step will be accepted. If the value is set to 1, only the code for the current time-step will be accepted. If it is increased, more time-steps each side of the current time-step will be accepted.

**Example** To set the window size to include codes for the two previous time-steps, the current, and the two time-steps following the current time (i.e. a total of 5 codes), use the commands:

```
awplus# configure terminal
awplus(config)# 2fa totp-window-size 5
```

To set the window size to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa totp-window-size
```

**Related commands**

- [2fa create user](#)
- [2fa delete user](#)
- [2fa hotp-window-size](#)
- [service 2fa](#)
- [show 2fa](#)
- [show 2fa user](#)
- [show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added

# 2fa self-registration port

**Overview** Use this command to enable Two-Factor Authentication (2FA) user self-registration and specify the HTTPS port.

Use the **no** variant of this command to disable 2FA user self-registration.

**Syntax** `2fa self-registration port <port-number>`  
`no 2fa self-registration`

| Parameter                        | Description                                                       |
|----------------------------------|-------------------------------------------------------------------|
| <code>&lt;port-number&gt;</code> | The port number from the range 1 to 65535. For example, port 443. |

**Default** Disabled

**Mode** Global Configuration

**Usage notes** The 2FA service must be running for this command to work. Use the [service 2fa](#) command to enable the 2FA service.

The port parameter allows the user to register on a specified port. A user can register by accessing the website hosted on the device at:  
`https://<device-ip>:<port>/2fa-registration`

The port specified in the command can be set to the same port as the port specified in the command [http secure-port](#), or the default secure port if one has not been set. However, it cannot be set to the HTTP port. The HTTP port is 80 by default, unless it has been changed with the command [http port](#).

Also, if PAC file hosting is enabled, then the user self-registration port must be set to a different port if it is not the same as the HTTP secure port.

While 2FA user self registration is disabled, the webpage is hidden. If someone tries to browse to it, they will see an error.

**Example** To enable 2FA user self-registration and specify the HTTPS port '443', use the commands:

```
awplus# configure terminal
awplus(config)# 2fa self-registration port 443
```

To disable 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# no 2fa self-registration
```

**Related commands** [service 2fa](#)

**Command  
changes**    Version 5.5.3-0.1: command added

# aaa authentication 2fa-registration default group

**Overview** Use this command to set authentication methods for Two-Factor Authentication (2FA) user self-registration.

Use the **no** variant of this command to unset authentication methods for 2FA user self-registration.

**Syntax** `aaa authentication 2fa-registration default group {ldap|radius|<group-name>}`

`no aaa authentication 2fa-registration default`

| Parameter    | Description                                                                               |
|--------------|-------------------------------------------------------------------------------------------|
| ldap         | Use all LDAP servers configured by the <b>ldap-server name</b> command.                   |
| radius       | Use all RADIUS servers configured by the <b>radius-server host</b> command.               |
| <group-name> | The name of the LDAP or RADIUS server group to authenticate self-registration users with. |

**Default** No servers are configured by default

**Mode** Global Configuration

**Examples** To configure LDAP servers to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group ldap
```

To configure RADIUS servers to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group radius
```

To configure a selected LDAP or RADIUS group of servers called 'GRP1' to authenticate the user for 2FA self-registration, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication 2fa-registration default
group GRP1
```

To remove the configured server group for 2FA self-registration to authenticate with, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no aaa authentication 2fa-registration default
```

**Related commands**    [2fa self-registration port](#)  
[service 2fa](#)

**Command changes**    Version 5.5.3-0.1: command added



# debug 2fa

**Overview** Use this command to turn on two-factor authentication (2FA) debug messaging.  
Use the **no** variant of this command to turn off 2FA debug messaging.

**Syntax** debug 2fa  
no debug 2fa

**Default** Debug messaging is turned off.

**Mode** Privileged Exec

**Example** To turn on 2FA debug messaging, use the command:

```
awplus# debug 2fa
```

**Related commands** [service 2fa](#)  
[show debugging 2fa](#)

**Command changes** Version 5.5.2-1.1: command added

# email-attribute (ldap-server)

**Overview** Use this command to set the attribute that the LDAP server stores user emails in for the Two-Factor Authentication One Time Password feature (2FA OTP). The attribute is used to retrieve the user email address that the 2FA OTP feature uses to email an OTP to the user.

Use the **no** variant of this command to set the attribute back to the default.

**Syntax** email-attribute <attribute-name>  
no email-attribute

| Parameter        | Description                                            |
|------------------|--------------------------------------------------------|
| <attribute-name> | LDAP mail attribute name. For example, UserCustomData. |

**Default** The default LDAP email attribute is userPrincipalName

**Mode** LDAP Server Configuration

**Examples** To set the attribute 'UserCustomData' as the email attribute for the LDAP server 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# email-attribute UserCustomData
```

To reset the attribute back to the default, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no email-attribute
```

**Output** Figure 38-10: Example output from **email-attribute**

```
email attribute changed.
```

**Related commands** [ldap-server](#)  
[2fa email-otp](#)

[2fa radius-email-attribute](#)

**Command changes** Version 5.5.3-0.1: command added

## service 2fa

**Overview** Use this command to enable Two-Factor Authentication (2FA).

2FA is a method of strengthening security by requiring a second method of authentication. AlliedWare Plus supports 2FA on OpenVPN connections. It requires a software-based authenticator that implements the time-based one-time password (TOTP) or HMAC-based one-time password (HOTP) algorithms.

These software authenticators (known as authenticator apps) are usually loaded on a mobile device. Google Authenticator is one well-known implementation of an authenticator app.

For more information on configuring 2FA on OpenVPN, see the “Two-factor authentication” chapter in the [OpenVPN Feature Overview and Configuration Guide](#).

Use the **no** variant of this command to disable 2FA.

**Syntax** `service 2fa`  
`no service 2fa`

**Default** Disabled

**Mode** Global Configuration

**Usage notes** Disabling the 2FA service stops the 2FA configuration from showing in the running configuration and prevents 2FA commands from working. You will not be able to view, create, or delete users with the service stopped. User data, however, is not deleted.

Additionally, the 2FA configuration is not reset until the device is rebooted. This means the configuration will be restored if the service is restarted before the device is rebooted.

If the OpenVPN method list is configured with 2FA and the 2FA service is not running, then two-factor authentication will be skipped and a critical message will be logged when a user connects.

**Example** To enable the 2FA service, use the command:

```
awplus# service 2fa
```

To disable the 2FA service, use the command:

```
awplus# no service 2fa
```

**Related commands** [2fa create user](#)  
[2fa delete user](#)

[show 2fa](#)

[show 2fa user](#)

[show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added

# show 2fa

**Overview** Use this command to display information about your Two-Factor Authentication (2FA) configuration and the status of the 2FA service.

**Syntax** `show 2fa`

**Mode** Privileged Exec

**Example** To display information on your 2FA configuration and status, use the command:

```
awplus# show 2fa
```

**Output** Figure 38-11: Example output from **show 2fa**

```
awplus#show 2fa

Settings:
 Allow TOTP code reuse: No
 Reject users with no config: No
 Allow user self-registration: On port 443
 TOTP window size: 3
 HOTP window size: 3
 Attempt Skew Adjustment: No
 Label: Unset (using hostname)
 Debug: Enabled
 Email OTP enabled: Yes

Number of configured users: 4
```

**Related commands**

- [2fa create user](#)
- [2fa delete user](#)
- [service 2fa](#)
- [show 2fa user](#)

**Command changes** Version 5.5.2-1.1: command added

# show 2fa email-template

**Overview** Use this command to display the email template used when sending Two-Factor Authentication One-Time-Passwords (2FA email OTP).

**Syntax** `show 2fa email-template`

**Mode** Privileged Exec

**Example** To display the email template used when sending OTPs, use the command:

```
awplus# show 2fa email-template
```

**Output** Figure 38-12: Example output from **show 2fa email-template**

```
Awplus#show 2fa email-template
Subject: %%LABEL%% 2FA Email OTP code

Verification code: %%OTP%%

The verification code will expire in %%EXPIRY_TIME%% minutes.
This is an automated message, please do not reply.
```

**Related commands** [2fa email-template](#)

**Command changes** Version 5.5.3-0.1: command added

# show 2fa user

**Overview** Use this command to display information about a Two-Factor Authentication (2FA) user. You can optionally display the user's QR code.

**Syntax** `show 2fa user <user-name> [qr {ansi|utf8|link}]`

| Parameter   | Description                                                                                                                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <user-name> | The name of the user you want to display.                                                                                                                                                                                            |
| qr          | Display the QR code.                                                                                                                                                                                                                 |
| ansi        | Display the QR code using ANSI block characters.                                                                                                                                                                                     |
| utf8        | Display the QR code using a UTF-8 mosaic.                                                                                                                                                                                            |
| link        | Display a hyperlink for a QR code generator. Opening the link in a browser will display a QR code. This option passes the string to an online QR code generator (at Google), so it may be a security concern for some installations. |

**Mode** Privileged Exec

**Usage notes** The QR code displays best in a color mode ANSI or UTF-8 terminal. If your terminal is insufficiently wide, or doesn't have the correct options enabled, you may not get a scannable QR code.

**Example1** To display 2FA information including the 2FA mode and the email address for the user name 'otp\_user1', use the command:

```
awplus# show 2fa user otp_user1
```

**Output 1** Figure 38-13: Example output from **show 2fa user otp\_user1**

```
awplus#show 2fa user otp_user1

Two-Factor Authentication information for user:

Username: otp_user1
Mode: Email
Email: otp_user1@xyz.com
```

**Example2** To display 2FA information, and display a hyperlink for a QR code generator, for user name 'test', use the command:

```
awplus# show 2fa user test qr link
```

**Output 2** Figure 38-14: Example output from **show 2fa user test qr link**

```
awplus#show 2fa user test qr link

Two-Factor Authentication information for user:

Username: test
Secret: RXB.....
Mode: TOTP
OTP URL: otpauth://totp/test@awplus?secret=RXB.....
Scratch codes:
 70344616
 91312817
 39931705
 89513481
 78647666

The following URL can be used to generate a QR code.
This results in the user key being sent to Google servers.
https://www.google.com/chart?chs=200x200&chld=M|0&cht=qr&chl=otpau
th://totp/test@awplus%3Fsecret%3DRXBH7KSCHOWZPG6JFBRROGPSY
```

**Related commands**

- [2fa create user email](#)
- [2fa create user](#)
- [2fa delete user](#)
- [service 2fa](#)
- [show 2fa](#)
- [show 2fa users](#)

**Command changes** Version 5.5.2-1.1: command added



# show 2fa users

**Overview** Use this command to display information about all the users configured with Two-Factor Authentication (2FA) on the device.

**Syntax** `show 2fa users`

**Mode** Privileged Exec

**Example** To display the information for all configured 2FA users, use the command:

```
awplus# show 2fa users
```

**Output** Figure 38-15: Example output from **show 2fa users**

```
awplus#show 2fa users
Two-Factor Authentication users:
Username Mode Last OTP Login

abcd Skip-2FA -
asasd Skip-2FA -
clientA1 TOTP -
clientA2 TOTP -
```

**Related commands**

- [2fa create user](#)
- [2fa delete user](#)
- [service 2fa](#)
- [show 2fa](#)
- [show 2fa user](#)

**Command changes** Version 5.5.2-1.1: command added

# show debugging 2fa

**Overview** Use this command to display debugging information for two-factor authentication (2FA).

**Syntax** `show debugging 2fa`

**Mode** Privileged Exec

**Example** To display debugging information for two-factor authentication, use the command:

```
awplus# show debugging 2fa
```

**Output** Figure 38-16: Example output from **show 2fa**

```
awplus# show debugging 2fa
2FA Debugging Status: on
```

**Related commands** [debug 2fa](#)  
[service 2fa](#)

**Command changes** Version 5.5.2-1.1: command added

# undebug 2fa

**Overview** Use this command to turn off debug messaging for Two-Factor Authentication (2FA).

**Syntax** `undebug 2fa`

**Default** 2FA debug messaging is off

**Mode** Privileged Exec

**Example** To turn off 2FA debug messaging, use the command:

```
awplus# undebug 2fa
```

**Related commands** [service 2fa](#)  
[show 2fa](#)

**Command changes** Version 5.5.3-0.1: command added

# 39

# Public Key Infrastructure and Crypto Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure the Public Key Infrastructure (PKI) capabilities on an AlliedWare Plus device. For more information about PKI, see the [Public Key Infrastructure \(PKI\) Feature Overview and Configuration Guide](#).

- Command List**
- ["crypto key generate rsa"](#) on page 1778
  - ["crypto key zeroize"](#) on page 1779
  - ["crypto pki authenticate"](#) on page 1780
  - ["crypto pki enroll"](#) on page 1781
  - ["crypto pki enroll user"](#) on page 1782
  - ["crypto pki export pem"](#) on page 1784
  - ["crypto pki export pkcs12"](#) on page 1785
  - ["crypto pki import pem"](#) on page 1787
  - ["crypto pki import pkcs12"](#) on page 1789
  - ["crypto pki trustpoint"](#) on page 1790
  - ["enrollment \(ca-trustpoint\)"](#) on page 1791
  - ["fingerprint \(ca-trustpoint\)"](#) on page 1792
  - ["no crypto pki certificate"](#) on page 1794
  - ["rsakeypair \(ca-trustpoint\)"](#) on page 1795
  - ["show crypto key mypubkey rsa"](#) on page 1796
  - ["show crypto pki certificates"](#) on page 1797
  - ["show crypto pki enrollment user"](#) on page 1799
  - ["show crypto pki trustpoint"](#) on page 1800
  - ["show hash"](#) on page 1801

- [“subject-name \(ca-trustpoint\)”](#) on page 1802

# crypto key generate rsa

**Overview** Use this command to generate a cryptographic public/private key pair for the Rivest-Shamir-Adleman (RSA) encryption algorithm.

**Syntax** `crypto key generate rsa [label <keylabel>] [<1024-16384>]`

| Parameter    | Description                                                                                                                                                                                                                                                                                 |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| label        | Specify and optional label for the key.                                                                                                                                                                                                                                                     |
| <keylabel>   | The name of the key to be created. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters. If no label is specified the default value "server-default" is used. |
| <1024-16384> | The bit length for the key. If no bit length is specified the default of 2048 is used.                                                                                                                                                                                                      |

**Mode** Privileged Exec

**Usage notes** The generated key may be used for multiple server certificates in the system. A key is referenced by its label. A bit length between 1024 and 16384 bits may be specified. Larger bit lengths are more secure, but require more computation time.  
The specified key must not already exist.

**Example** To create a key with the label 'example-server-key' and a bit length of 4096, use the commands:

```
awplus> enable
awplus# crypto key generate rsa label example-server-key 4096
```

**Related commands** [crypto key zeroize](#)  
[rsakeypair \(ca-trustpoint\)](#)  
[show crypto key mypubkey rsa](#)

**Command changes** Version 5.5.2-2.1: Key length increased to 16384

# crypto key zeroize

**Overview** Use this command to delete one or all cryptographic public/private key pairs.

**Syntax** `crypto key zeroize rsa <keylabel>`  
`crypto key zeroize all`

| Parameter                         | Description                                                                        |
|-----------------------------------|------------------------------------------------------------------------------------|
| <code>rsa &lt;keylabel&gt;</code> | Delete a single key pair for the Rivest-Shamir-Adleman (RSA) encryption algorithm. |
| <code>all</code>                  | Delete all keys.                                                                   |

**Mode** Privileged Exec

**Usage notes** Note that this command has the same effect as using the **delete** command (it deletes the file from Flash memory but does not overwrite it with zeros).  
The specified key must exist but must not be in use for any existing server certificates.  
A key may not be deleted if it is associated with the server certificate or server certificate signing request for an existing trustpoint. To remove a server certificate so that the key may be deleted, use the **no crypto pki enroll** command to de-enroll the server.

**Example** To delete an RSA key named "example-server-key", use the following command:

```
awplus# crypto key zeroize rsa example-server-key
```

**Related commands** [crypto key generate rsa](#)  
[show crypto key mypubkey rsa](#)

**Command changes** Version 5.4.6-1.1: zeroize functionality added to x930 Series  
Version 5.4.8-1.2: zeroize functionality added to x220, XS900MX, x550 Series  
Version 5.4.8-2.1: zeroize functionality added to SBx908 GEN2, x950 Series

# crypto pki authenticate

**Overview** Use this command to authenticate a trustpoint by generating or importing the root CA certificate. This must be done before the server can be enrolled to the trustpoint.

**Syntax** `crypto pki authenticate <trustpoint>`

| Parameter    | Description                                     |
|--------------|-------------------------------------------------|
| <trustpoint> | The name of the trustpoint to be authenticated. |

**Mode** Privileged Exec

**Usage notes** If the trustpoint's **enrollment** setting is "selfsigned", then this command causes a private key to be generated for the root CA, and a self-signed certificate to be generated based on that key.

If the trustpoint's **enrollment** setting is "terminal", then this command prompts the user to paste a certificate Privacy Enhanced Mail (PEM) file at the CLI terminal. If the certificate is a valid selfsigned CA certificate, then it will be stored as the trustpoint's root CA certificate.

The specified trustpoint must already exist, and its enrollment mode must have been defined.

**Example** To show the **enrollment** setting of a trustpoint named "example" and then generate a certificate from it, use the commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# enrollment selfsigned
awplus(config)# exit
awplus# exit
awplus# crypto pki authenticate example
```

**Related commands** [crypto pki import pem](#)  
[crypto pki trustpoint](#)  
[enrollment \(ca-trustpoint\)](#)



# crypto pki enroll

**Overview** Use this command to enroll the local server to the specified trustpoint.  
Use the **no** variant of this command to de-enroll the server by removing its certificate

**Syntax** `crypto pki enroll <trustpoint>`  
`no crypto pki enroll <trustpoint>`

| Parameter                       | Description                               |
|---------------------------------|-------------------------------------------|
| <code>&lt;trustpoint&gt;</code> | The name of the trustpoint to be enrolled |

**Mode** Privileged Exec

**Usage notes** For the local server, “enrollment” is the process of creating of a certificate for the server that has been signed by a CA associated with the trustpoint. The public portion of the RSA key pair specified using the `rsakeypair` parameter for the trustpoint will be included in the server certificate.

If the trustpoint represents a locally self-signed certificate authority, then this command results in the direct generation of the server certificate, signed by the root CA for the trustpoint.

If the trustpoint represents an external certificate authority, then this command results in the generation of a Certificate Signing Request (CSR) file, which is displayed at the terminal in Privacy-Enhanced Mail (PEM) format, suitable for copying and pasting into a file or message. The CSR must be sent to the external CA for processing. When the CA replies with the signed certificate, that certificate should be imported using the `crypto pki import pem` command, to complete the enrollment process.

The specified trustpoint must already exist, and it must already be authenticated.

**Example** To enroll the local server with the trustpoint “example”, use the following commands:

```
awplus> enable
awplus# crypto pki enroll example
```

**Related commands** [crypto pki enroll user](#)  
[crypto pki import pem](#)  
[crypto pki trustpoint](#)  
[enrollment \(ca-trustpoint\)](#)

# crypto pki enroll user

**Overview** Use this command to enroll a single RADIUS user or all RADIUS users to the specified trustpoint.

Use the **no** variant of this command to remove the PKCS#12 file from the system. Note that the PKCS#12 files are generated in a temporary (volatile) file system, so a system restart also results in removal of all of the files.

**Syntax**

```
crypto pki enroll <trustpoint>
{user <username>|local-radius-all-users}

no crypto pki enroll <trustpoint>
{user <username>|local-radius-all-users}
```

| Parameter    | Description                                                   |
|--------------|---------------------------------------------------------------|
| <trustpoint> | The name of the trustpoint to which users are to be enrolled. |
| <username>   | The name of the user to enroll to the trustpoint.             |

**Mode** Privileged Exec

**Usage notes** For RADIUS users, “enrollment” is the process of generating a private key and a corresponding client certificate for each user, with the certificate signed by the root CA for the trustpoint. The resulting certificates may be exported to client devices, for use with PEAP or EAP-TLS authentication with the local RADIUS server.

The specified trustpoint must represent a locally self-signed certificate authority.

The private key and certificate are packaged into a PKCS#12-formatted file, suitable for export using the **crypto pki export pkcs12** command. The private key is encrypted for security, with a passphrase that is entered at the command line. The passphrase is required when the PKCS#12 file is imported on the client system. The passphrase is not stored anywhere on the device, so users are responsible for remembering it until the export-import process is complete.

If **local-radius-all-users** is specified instead of an individual user, then keys and certificates for all RADIUS users will be generated at once. All the keys will be encrypted using the same passphrase.

The specified trustpoint must already exist, it must represent a locally self-signed CA, and it must already have been authenticated.

**Example** To enroll the user “example-user” with the trustpoint “example”, use the following commands:

```
awplus> enable
awplus# crypto pki enroll example user example-user
```

To enroll all local RADIUS users with the trustpoint “example”, use the following commands:

```
awplus> enable
```

```
awplus# crypto pki enroll example local-radius-all-users
```

**Related  
commands**

[crypto pki export pkcs12](#)

[crypto pki trustpoint](#)

# crypto pki export pem

**Overview** Use this command to export the root CA certificate for the given trustpoint to a file in Privacy-Enhanced Mail (PEM) format. The file may be transferred to the specified destination URL, or displayed at the terminal.

**Syntax** `crypto pki export <trustpoint> pem [terminal|<url>]`

| Parameter    | Description                                                                     |
|--------------|---------------------------------------------------------------------------------|
| <trustpoint> | The name of the trustpoint for which the root CA certificate is to be exported. |
| terminal     | Display the PEM file to the terminal.                                           |
| <url>        | Transfer the PEM file to the specified URL.                                     |

**Default** The PEM will be displayed to the terminal by default.

**Mode** Privileged Exec

**Usage notes** The specified trustpoint must already exist, and it must already be authenticated.

**Example** To display the PEM file for the trustpoint "example" to the terminal, use the following commands:

```
awplus> enable
awplus# crypto pki export example pem terminal
```

To export the PEM file "example.pem" for the trustpoint "example" to the URL "tftp://server\_a/", use the following commands:

```
awplus> enable
awplus# crypto pki export example pem
tftp://server_a/example.pem
```

**Related commands**

- [crypto pki authenticate](#)
- [crypto pki import pem](#)
- [crypto pki trustpoint](#)

# crypto pki export pkcs12

**Overview** Use this command to export a certificate and private key for an entity in a trustpoint to a file in PKCS#12 format at the specified URL. The private key is encrypted with a passphrase for security.

**Syntax** `crypto pki export <trustpoint> pkcs12 {ca|server|<username>} <url>`

| Parameter    | Description                                                                                                                                                                                                                                        |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <trustpoint> | The name of the trustpoint for which the certificate and key are to be exported.                                                                                                                                                                   |
| ca           | If this option is specified, the command exports the root CA certificate and corresponding key.                                                                                                                                                    |
| server       | If this option is specified, the command exports the server certificate and corresponding key.                                                                                                                                                     |
| <username>   | If a RADIUS username is specified, the command exports the PKCS#12 file that was previously generated using the <code>crypto pki enroll user</code> command. To avoid ambiguity with keywords, the username may be prefixed by the string "user:". |
| <url>        | The destination URL for the PKCS#12 file. The format of the URL is the same as any valid destination for a file copy command.                                                                                                                      |

**Mode** Privileged Exec

**Usage notes** If the **ca** option is specified, this command exports the root CA certificate and the corresponding private key, if the trustpoint has been authenticated as a locally selfsigned CA. (If the trustpoint represents an external CA, then there is no private key on the system corresponding to the root CA certificate. Use the **crypto pki export pem** file to export the certificate by itself.) The command prompts for a passphrase to encrypt the private key.

If the **server** option is specified, this command exports the server certificate and the corresponding private key, if the server has been enrolled to the trustpoint. The command prompts for a passphrase to encrypt the private key.

If a RADIUS username is specified, this command exports the PKCS#12 file that was generated using the **crypto pki enroll user** command. (The key within the file was already encrypted as part of the user enrollment process.)

In the event that there is a RADIUS user named "ca" or "server", enter "user:ca" or "user:server" as the username.

The key and certificate must already exist.

**Example** To export the PKCS#12 file "example.pk12" for the trustpoint "example" to the URL "tftp://backup/", use the following commands:

```
awplus> enable

awplus# crypto pki export example pkcs12 ca
tftp://backup/example.pk12
```

**Related commands**

- crypto pki enroll user
- crypto pki export pem
- crypto pki import pkcs12

# crypto pki import pem

**Overview** This command imports a certificate for the given trustpoint from a file in Privacy-Enhanced Mail (PEM) format. The file may be transferred from the specified destination URL, or entered at the terminal.

**Syntax** `crypto pki import <trustpoint> pem [terminal|<url>]`

| Parameter    | Description                                                                                                                                                                |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <trustpoint> | The name of the trustpoint for which the root CA certificate is to be imported.                                                                                            |
| terminal     | Optional parameter, If specified, the command prompts the user to enter (or paste) the PEM file at the terminal. If parameter is specified terminal is assumed by default. |
| <url>        | Optional parameter, If specified, the PEM file is transferred from the specified URL                                                                                       |

**Default** The PEM will be imported from the terminal by default.

**Mode** Privileged Exec

**Usage notes** The command is generally used for trustpoints representing external certificate authorities. It accepts root CA certificates, intermediate CA certificates, and server certificates. The system automatically detects the certificate type upon import.

Using this command to import root CA certificates at the terminal is identical to the functionality provided by the `crypto pki authenticate` command, for external certificate authorities. The imported certificate is validated to ensure it is a proper CA certificate.

Intermediate CA certificates are validated to ensure they are proper CA certificates, and that the issuer chain ends in a root CA certificate already installed for the trustpoint. If there is no root CA certificate for the trustpoint (i.e., if the trustpoint is unauthenticated) then intermediate CA certificates may not be imported.

Server certificates are validated to ensure that the issuer chain ends in a root CA certificate already installed for the trustpoint. If there is no root CA certificate for the trustpoint (i.e., if the trustpoint is unauthenticated) then server certificates may not be imported.

The specified trustpoint must already exist. If the imported certificate is self-signed, then no certificates may exist for the trustpoint. Otherwise, the issuer's certificate must already be present for the trustpoint.

**Example** To import the PEM file for the trustpoint "example" from the terminal, use the following commands:

```
awplus> enable
awplus# crypto pki import example pem
```

To import the PEM file for the trustpoint “example” from the URL “tftp://server\_a/”, use the following commands:

```
awplus> enable
awplus# crypto pki import example pem
tftp://server_a/example.pem
```

**Related  
commands**

[crypto pki authenticate](#)  
[crypto pki export pem](#)  
[crypto pki trustpoint](#)



# crypto pki import pkcs12

**Overview** This command imports a certificate and private key for an entity in a trustpoint from a file in PKCS#12 format at the specified URL. The command prompts for a passphrase to decrypt the private key within the file.

**Syntax** `crypto pki import <trustpoint> pkcs12 {ca|server} <url>`

| Parameter    | Description                                                                                                              |
|--------------|--------------------------------------------------------------------------------------------------------------------------|
| <trustpoint> | The name of the trustpoint for which the certificate and key are to be imported.                                         |
| ca           | If this option is specified, the command imports the root CA certificate and corresponding key.                          |
| server       | If this option is specified, the command imports the server certificate and corresponding key.                           |
| <url>        | The source URL for the PKCS#12 file. The format of the URL is the same as any valid destination for a file copy command. |

**Mode** Privileged Exec

**Usage notes** If the **ca** option is specified, this command imports the root CA certificate and the corresponding private key. This is only valid if the root CA certificate does not already exist for the trustpoint (i.e., if the trustpoint is unauthenticated).

If the **server** option is specified, this command imports the server certificate and the corresponding private key. The imported private key is given a new unique label of the form "localN", where N is a non-negative integer. This operation is only valid if the server certificate does not already exist for the trustpoint (i.e., if the server is not enrolled to the trustpoint).

PKCS#12 files for RADIUS users may not be imported with this command. (There is no value in doing so, as the files are not needed on the local system.)

The specified trustpoint must already exist. The key and certificate must not already exist.

**Example** To import the PKCS#12 file "example.pk12" for the trustpoint "example" to the URL "tftp://backup/", use the following commands:

```
awplus> enable
awplus# crypto pki import example pkcs12 ca
tftp://backup/example.pk12
```

**Related commands** [crypto pki export pkcs12](#)  
[crypto pki import pem](#)

# crypto pki trustpoint

**Overview** Use this command to declare the named trustpoint and enter trustpoint configuration mode.

Use the **no** variant of this command to destroy the trustpoint.

**Syntax** `crypto pki trustpoint <trustpoint>`  
`no crypto pki trustpoint <trustpoint>`

| Parameter    | Description                                                                                                                                                                                                     |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <trustpoint> | The name of the trustpoint. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters. |

**Mode** Global Configuration

**Usage notes** If the trustpoint did not previously exist, it is created as a new trustpoint. The trustpoint will be empty (unauthenticated) unless the name “local” is selected, in which case the system will automatically authenticate the trustpoint as a local self-signed certificate authority.

The **no** variant of this command destroys the trustpoint by removing all CA and server certificates associated with the trustpoint, as well as the private key associated with the root certificate (if the root certificate was locally self-signed). This is a destructive and irreversible operation, so this command should be used with caution.

**Example** To configure a trustpoint named “example”, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
```

**Related commands** [show crypto pki certificates](#)  
[show crypto pki trustpoint](#)

**Command changes** Version 5.4.6-1.1: command added to x930 Series  
Version 5.4.8-1: command added to x220, XS900MX, x550 Series  
Version 5.4.8-2.1: command added to SBx908 GEN2, x950 Series

# enrollment (ca-trustpoint)

**Overview** Use this command to declare how certificates will be added to the system for the current trustpoint.

**Syntax** `enrollment {selfsigned|terminal}`

| Parameter               | Description                                                        |
|-------------------------|--------------------------------------------------------------------|
| <code>selfsigned</code> | Sets the enrollment mode for the current trustpoint to selfsigned. |
| <code>terminal</code>   | Sets the enrollment mode for the current trustpoint to terminal.   |

**Mode** Trustpoint Configuration

**Usage notes** If the enrollment is set to **selfsigned**, then the system will generate a root CA certificate and its associated key when the **crypto pki authenticate** command is issued. It will generate a server certificate (signed by the root CA certificate) when the **crypto pki enroll** command is issued.

If the enrollment is set to **terminal**, then the system will prompt the user to paste the root CA certificate Privacy Enhanced Mail (PEM) file at the terminal, when the **crypto pki authenticate** command is issued. It will create a Certificate Signing Request (CSR) file for the local server when the **crypto pki enroll** command is issued. The server certificate received from the external CA should be imported using the **crypto pki import pem** command.

The trustpoint named "local" may only use the **selfsigned** enrollment setting.

If no enrollment mode is specified, the **crypto pki authenticate** command will fail for the trustpoint.

**Example** To configure the trustpoint named "example" and set its enrollment to **selfsigned**, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# enrollment selfsigned
```

**Related commands** [crypto pki enroll](#)

# fingerprint (ca-trustpoint)

**Overview** Use this command to declare that certificates with the specified fingerprint should be automatically accepted, when importing certificates from an external certificate authority. This can affect the behavior of the **crypto pki authenticate** and **crypto pki import pem** commands.

Use the **no** variant of this command to remove the specified fingerprint from the pre-accepted list.

**Syntax** fingerprint <word>  
no fingerprint <word>

| Parameter | Description                                                                                                     |
|-----------|-----------------------------------------------------------------------------------------------------------------|
| <word>    | The fingerprint as a series of 40 hexadecimal characters, optionally separated into multiple character strings. |

**Default** By default, no fingerprints are pre-accepted for the trustpoint.

**Mode** Trustpoint Configuration

**Usage notes** Specifying a fingerprint adds it to a list of pre-accepted fingerprints for the trustpoint. When a certificate is imported, if it matches any of the pre-accepted values, then it will be saved in the system automatically. If the imported certificate's fingerprint does not match any pre-accepted value, then the user will be prompted to verify the certificate contents and fingerprint visually.

This command is useful when certificates from an external certificate authority are being transmitted over an insecure channel. If the certificate fingerprint is delivered via a separate messaging channel, then pre-entering the fingerprint value via cut-and-paste may be less errorprone than attempting to verify the fingerprint value visually.

The fingerprint is a series of 40 hexadecimal characters. It may be entered as a continuous string, or as a series of up to multiple strings separated by spaces. The input format is flexible because different certificate authorities may provide the fingerprint string in different formats.

**Example** To configure a fingerprint "5A81D34C 759CC4DA CFCA9F65 0303AD83 410B03AF" for the trustpoint named "example", use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# fingerprint 5A81D34C 759CC4DA CFCA9F65
0303AD83 410B03AF
```

**Related commands** [crypto pki authenticate](#)

`crypto pki import pem`

# no crypto pki certificate

**Overview** Use this command to delete a certificate with the specified fingerprint from the specified trustpoint.

**Syntax** no crypto pki certificate *<trustpoint>* *<word>*

| Parameter                 | Description                                                                                                     |
|---------------------------|-----------------------------------------------------------------------------------------------------------------|
| <i>&lt;trustpoint&gt;</i> | The name of the trustpoint.                                                                                     |
| <i>&lt;word&gt;</i>       | The fingerprint as a series of 40 hexadecimal characters, optionally separated into multiple character strings. |

**Default** By default, no fingerprints are pre-accepted for the trustpoint.

**Mode** Privileged Exec

**Usage notes** The fingerprint can be found in the output of the **show crypto pki certificates** command. If there are dependent certificates in the trustpoint (i.e., if other certificates were signed by the specified certificate), the command will be rejected.

If the specified certificate is the root CA certificate and the trustpoint represents a locally selfsigned CA, then the corresponding private key is also deleted from the system. Deleting the root CA certificate effectively resets the trustpoint to an unauthenticated state.

**Example** To delete a certificate with the fingerprint "594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792" from the trustpoint "example", use the following commands:

```
awplus> enable
awplus# no crypto pki certificate example
594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792
```

**Related commands** [no crypto pki trustpoint](#)  
[show crypto pki certificates](#)

# rsakeypair (ca-trustpoint)

**Overview** Use this command to declare which RSA key pair should be used to enroll the local server with the trustpoint. Note that this defines the key pair used with the server certificate, not the key pair used with the root CA certificate.

Use the **no** variant of this command to restore the default value, "server-default".

**Syntax** `rsakeypair <keylabel> [<1024-4096>]`  
`no rsakeypair`

| Parameter                      | Description                                                                                                                                                                                                                                             |
|--------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;keylabel&gt;</code>  | The key to be used with the server certificate for this trustpoint. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters. |
| <code>&lt;1024-4096&gt;</code> | The bit length for the key, to be used if the key is implicitly generated during server enrollment.                                                                                                                                                     |

**Default** The default value for **keylabel** is "server-default".  
The default value for the key bit length is 2048.

**Mode** Trustpoint Configuration

**Usage notes** If the label specified does not refer to an existing key created by the **crypto key generate rsa** command, the key will be implicitly generated when the **crypto pki enroll** command is issued to generate the server certificate or the server certificate signing request. The optional numeric parameter defines the bit length for the key, and is only applicable for keys that are implicitly created during enrollment.

This command does not affect server certificates or server certificate signing requests that have already been generated. The trustpoint's server certificate is set to use whatever key pair was specified for the trustpoint at the time the **crypto pki enroll** command is issued.

The default key pair is "server-default". The default bit length is 2048 bits.

**Example** To configure trustpoint "example" to use the key pair "example-server-key" with a bit length of 2048, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# rsakeypair example-server-key 2048
```

**Related commands** [crypto key generate rsa](#)

# show crypto key mypubkey rsa

**Overview** Use this command to display information about the specified Rivest-Shamir-Adleman encryption key.

**Syntax** `show crypto key mypubkey rsa [<keylabel>]`

| Parameter  | Description                                    |
|------------|------------------------------------------------|
| <keylabel> | The name of the key to be shown, if specified. |

**Default** By default, all keys will be shown.

**Mode** Privileged Exec

**Usage notes** If no key label is specified, information about all keys is shown. The command displays the bit length of the key, a key fingerprint (a hash of the key contents to help uniquely identify a key), and a list of trustpoints in which the server certificate is using the key.

The specified keys must exist.

**Example** To show all keys, use the following commands:

```
awplus> enable
awplus# show crypto key mypubkey rsa
```

**Output** Figure 39-1: Example output from **show crypto key mypubkey rsa**

```
awplus#show crypto key mypubkey rsa

RSA Key Pair "example-server-key":
 Key size : 2048 bits
 Fingerprint : 1A605D73 C2274CB7 853886B3 1C802FC6 7CDE45FB
 Trustpoints : example

RSA Key Pair "server-default":
 Key size : 2048 bits
 Fingerprint : 34AC4D2D 5249A168 29D426A3 434FFC59 C4A19901
 Trustpoints : local
```

**Related commands** [crypto key generate rsa](#)



# show crypto pki certificates

**Overview** Use this command to display information about existing certificates for the specified trustpoint.

**Syntax** `show crypto pki certificates [<trustpoint>]`

| Parameter                       | Description                                                |
|---------------------------------|------------------------------------------------------------|
| <code>&lt;trustpoint&gt;</code> | The trustpoint for which the certificates are to be shown. |

**Default** By default, the certificates for all trustpoints are shown.

**Mode** Privileged Exec

**Usage notes** If no trustpoint is specified, certificates for all trustpoints are shown. The command displays the certificates organized into certificate chains. It starts with the server certificate and then displays its issuer, and continues up the issuer chain until the root CA certificate is reached.

For each certificate, the command displays the certificate type, the subject's distinguished name (the entity identified by the certificate), the issuer's distinguished name (the entity that signed the certificate), the validity dates for the certificate, and the fingerprint of the certificate. The fingerprint is a cryptographic hash of the certificate contents that uniquely identifies the certificate.

The specified trustpoints must already exist.

**Example** To show the certificates for the trustpoint "example", use the following command:

```
awplus> enable
awplus# show crypto pki certificates example
```

**Output** Figure 39-2: Example output from **show crypto pki certificates**

```
awplus>enable
awplus#show crypto pki certificates example

Trustpoint "example" Certificate Chain

Server certificate
 Subject : /O=local/CN=local.loc.lc
 Issuer : /C=NZ/CN=local_Signing_CA
 Valid From : Nov 11 15:35:21 2015 GMT
 Valid To : Aug 31 15:35:21 2018 GMT
 Fingerprint : 5A81D34C 759CC4DA CFCA9F65 0303AD83 410B03AF
Intermediate CA certificate
 Subject : /C=NZ/CN=example_Signing_CA
 Issuer : /C=NZ/CN=example_Root_CA
 Valid From : Sep 3 18:45:01 2015 GMT
 Valid To : Oct 10 18:45:01 2020 GMT
 Fingerprint : AE2D5850 9867D258 ABBEE95E 2E0E3D81 60714920
Imported root certificate
 Subject : /C=NZ/CN=example_Root_CA
 Issuer : /C=NZ/CN=example_Root_CA
 Valid From : Jul 23 18:12:10 2015 GMT
 Valid To : May 12 18:12:10 2025 GMT
 Fingerprint : 594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792
```

**Related commands** [crypto pki trustpoint](#)

# show crypto pki enrollment user

**Overview** Use this command to display a list of trustpoints for which RADIUS user enrollments have been performed, using the **crypto pki enroll user** command. This indicates that PKCS#12 files for the user are available for export for the given trustpoints, using the **crypto pki export pkcs12** command.

**Syntax** `crypto pki enrollment user <username>`

| Parameter  | Description                                     |
|------------|-------------------------------------------------|
| <username> | The user for which enrollments are to be shown. |

**Mode** Privileged Exec

**Example** To show the list of trustpoints to which user "exampleuser1" is enrolled, use the following commands:

```
awplus> enable
awplus(config)# show crypto pki enrollment user exampleuser1
```

**Output** Figure 39-3: Example output from **show crypto pki enrollment user**

```
awplus> enable
awplus# show crypto pki enrollment user exampleuser1
User "exampleuser1" is enrolled to the following trustpoints:
local,example
```

**Related commands** [crypto pki enroll user](#)  
[crypto pki export pkcs12](#)

# show crypto pki trustpoint

**Overview** Use this command to display information about the specified trustpoint.

**Syntax** `show crypto pki trustpoint [<trustpoint>]`

| Parameter    | Description                            |
|--------------|----------------------------------------|
| <trustpoint> | The name of the trustpoint to be shown |

**Default** By default, all trustpoints are shown.

**Mode** Privileged Exec

**Usage notes** If no trustpoint is specified, information about all trustpoints is shown. The command displays the authentication status of the trustpoint, the fingerprint of the root CA certificate (if it exists), the enrollment status of the local server with the trustpoint, a list of any applications that are configured to use the trustpoint, and the trustpoint parameters that were configured from trustpoint-configuration mode.

The specified trustpoints must already exist.

**Example** To show the details of the trustpoint "example", use the following commands:

```
awplus> enable
awplus# show crypto pki trustpoint example
```

**Output** Figure 39-4: Example output from **show crypto pki trustpoint**

```
awplus> enable
awplus# show crypto pki trustpoint example

Trustpoint "example"
 Type : Self-signed certificate authority
 Root Certificate: 50C1856B EEC7555A 0F3A61F6 690D9463 67DF74D1
 Local Server : The server is enrolled to this trustpoint.
 Server Key : example-server-key
 Applications : RADIUS

Authentication and Enrollment Parameters:
 Enrollment : selfsigned
 RSA Key Pair : example-server-key (2048 bits)

```

**Related commands** [crypto pki trustpoint](#)  
[show crypto pki certificates](#)

# show hash

**Overview** Use this command to display the hash for a specified file on the device.

**Syntax** `show hash <filename>`

| Parameter                     | Description                                   |
|-------------------------------|-----------------------------------------------|
| <code>&lt;filename&gt;</code> | The name of the file to display the hash for. |

**Mode** Privileged Exec

**Examples** To show the hash for the GUI file named `awplus-gui_552_27.gui`, use the command:

```
awplus# show hash awplus-gui_552_27.gui
```

To show the hash for a file named 'example.txt', which is in the folder named 'example' in flash memory, use the command:

```
awplus# show hash flash://example/example.txt
```

**Output** Figure 39-5: Example output from **show hash**

```
awplus#show hash awplus-gui_552_27.gui
b793e2c7fc5580513472017f964316f3bb0e79fbf1ddfd6f3844a2a8311c5c64
```

**Command changes** Version 5.5.3-0.1: command added

# subject-name (ca-trustpoint)

**Overview** Use this command to specify the distinguished name string that should be used for the subject field in the server certificate, when enrolling the server (generating the server certificate or server certificate signing request).

**Syntax** `subject-name <word>`

| Parameter                 | Description                                                                                                                                                   |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;word&gt;</code> | Specify the subject name as a distinguished name string. Complex strings (e.g., strings containing spaces) should be surrounded with double-quote characters. |

**Default** If no subject name is specified for the trustpoint, then the system automatically builds a name of the form `/O=AlliedWare Plus/CN=xxxx.yyyy.zzz`, where `xxxx` is the hostname of the system and `yyyy.zzz` is the default search domain for the system.

**Mode** Trustpoint Configuration

**Usage notes** The subject name is specified as a variable number of fields, where each field begins with a forward-slash character (`/`). Each field is of the form `XX=value`, where `XX` is the abbreviation of the node type in the tree.

Common values include:

- `"C"` (country),
- `"ST"` (state),
- `"L"` (locality),
- `"O"` (organization),
- `"OU"` (organizational unit), and
- `"CN"` (common name).

Of these fields, `"CN"` is usually the most important.

**NOTE:** For a server certificate, many applications require that the network name of the server matches the common name in the server's certificate.

**Example** To configure the trustpoint named "example" and set its subject name, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# subject-name "/O=My
Company/CN=192.168.1.1
```

**Related** `crypto pki enroll`  
**commands**

# 40

# TACACS+ Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure the device to use TACACS+ servers. For more information about TACACS+, see the [TACACS+ Feature Overview and Configuration Guide](#).

- Command List**
- [“aaa authorization commands”](#) on page 1805
  - [“aaa authorization config-commands”](#) on page 1807
  - [“authorization commands”](#) on page 1808
  - [“ip tacacs source-interface”](#) on page 1810
  - [“show tacacs+”](#) on page 1811
  - [“tacacs-server host”](#) on page 1813
  - [“tacacs-server key”](#) on page 1815
  - [“tacacs-server timeout”](#) on page 1816



# aaa authorization commands

**Overview** This command configures a method list for commands authorization that can be applied to console or VTY lines. When command authorization is enabled for a privilege level, only authorized users can executed commands in that privilege level.

Use the **no** variant of this command to remove a named method list or disable the default method list for a privilege level.

**Syntax**

```
aaa authorization commands <privilege-level>
{default|<list-name>} group tacacs+ [none]

no aaa authorization commands <privilege-level>
{default|<list-name>}
```

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <privilege-level> | The privilege level of the set of commands the method list will be applied to.<br>AlliedWare Plus defines three sets of commands, that are indexed by a level value:<br><b>Level = 1:</b> All commands that can be accessed by a user with privilege level between 1 and 6 inclusive<br><b>Level = 7:</b> All commands that can be accessed by a user with privilege level between 7 and 14 inclusive<br><b>Level = 15:</b> All commands that can be accessed by a user with privilege level 15 |
| group             | Specify the server group where authorization messages are sent. Only the <code>tacacs+</code> group is available for this command.                                                                                                                                                                                                                                                                                                                                                              |
| tacacs+           | Use all TACACS+ servers configured by the <code>tacacs-server host</code> command.                                                                                                                                                                                                                                                                                                                                                                                                              |
| default           | Configure the default authorization commands method list.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <list-name>       | Configure a named authorization commands method list                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| none              | If specified, this provides a local fallback to command authorization so that if authorization servers become unavailable then the device will accept all commands normally allowed for the privilege level of the user.                                                                                                                                                                                                                                                                        |

**Mode** Global Configuration

**Usage notes** TACACS+ command authorization provides centralized control of the commands available to a user of an AlliedWare Plus device. Once enabled:

- The command string and username are encrypted and sent to the first available configured TACACS+ server (the first server configured) for authorization.

- The TACACS+ server decides if the user is authorized to execute the command and returns the decision to the AlliedWare Plus device.
- Depending on this decision the device will then either execute the command or notify the user that authorization has failed.

If multiple TACACS+ servers are configured, and the first server is unreachable or does not respond, the other servers will be queried, in turn, for an authorization decision. If all servers are unreachable and a local fallback has been configured, with the **none** parameter, then commands are authorized based on the user's privilege level; the same behavior as if command authorization had not been configured. If, however, the local fallback is not configured and all servers become unreachable then all commands except **logout**, **exit**, and **quit** will be denied.

The **default** method list is defined with a local fallback unless configured differently using this command.

**Example** To configure a commands authorization method list, named TAC15, using all TACACS+ servers to authorize commands for privilege level 15, with a local fallback, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authorization commands 15 TAC15 group
tacacs+ none
```

To configure the default method list to authorize commands for privilege level 7, with no local fallback, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authorization commands 7 default group
tacacs+
```

To remove the authorization method list TAC15, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authorization commands 15 TAC15
```

**Related commands** [aaa authorization config-commands](#)  
[authorization commands](#)  
[tacacs-server host](#)

**Command changes** Version 5.4.6-2.1: command added

# aaa authorization config-commands

**Overview** Use this command to enable command authorization on configuration mode commands. By default, command authorization applies to commands in exec mode only.

Use the **no** variant of this command to disable command authorization on configuration mode commands.

**Syntax** `aaa authorization config-commands`  
`no aaa authorization config-commands`

**Default** By default, command authorization is disabled on configuration mode commands.

**Mode** Global Configuration

**Usage notes** If authorization of configuration mode commands is not enabled then all configuration commands are accepted by default, including command authorization commands.

**NOTE:** *Authorization of configuration commands is required for a secure TACACS+ command authorization configuration as it prevents the feature from being disabled to gain access to unauthorized exec mode commands.*

**Example** To enable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authorization config-commands
```

To disable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authorization config-commands
```

**Related commands** [aaa authorization commands](#)  
[authorization commands](#)  
[tacacs-server host](#)

**Command changes** Version 5.4.6-2.1: command added

# authorization commands

**Overview** This command applies a command authorization method list, defined using the [aaa authorization commands](#) command, to console and VTY lines.

Use the **no** variant of this command to reset the command authorization configuration on the console and VTY lines.

**Syntax** `authorization commands <privilege-level> {default|<list-name>}`  
`no authorization commands <privilege-level>`

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <privilege-level> | The privilege level of the set of commands the method list will be applied to.<br>AlliedWare Plus defines three sets of commands, that are indexed by a level value:<br><b>Level = 1:</b> All commands that can be accessed by a user with privilege level between 1 and 6 inclusive<br><b>Level = 7:</b> All commands that can be accessed by a user with privilege level between 7 and 14 inclusive<br><b>Level = 15:</b> All commands that can be accessed by a user with privilege level 15 |
| default           | Configure the default authorization commands method list.                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <list-name>       | Configure a named authorization commands method list                                                                                                                                                                                                                                                                                                                                                                                                                                            |

**Default** The **default** method list is applied to each console and VTY line by default.

**Mode** Line Configuration

**Usage notes** If the specified method list does not exist users will not be able to execute any commands in the specified method list on the specified VTY lines.

**Example** To apply the TAC15 command authorization method list with privilege level 15 to VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# authorization commands 15 TAC15
```

To reset the command authorization configuration with privilege level 15 on VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# no authorization commands 15
```

**Related commands** [aaa authorization commands](#)

aaa authorization config-commands

tacacs-server host

**Command  
changes**

Version 5.4.6-2.1: command added

# ip tacacs source-interface

**Overview** This command sets the source interface, or IP address, to use for all TACACS+ packets sent from the device. By default, TACACS+ packets use the source IP address of the egress interface.

Use the **no** variant of this command to remove the source interface configuration and use the source IP address of the egress interface.

**Syntax** `ip tacacs source-interface {<interface>|<ip-address>}`  
`no ip tacacs source-interface`

| Parameter                       | Description                                      |
|---------------------------------|--------------------------------------------------|
| <code>&lt;interface&gt;</code>  | Interface name.                                  |
| <code>&lt;ip-address&gt;</code> | IP address in the dotted decimal format A.B.C.D. |

**Default** The source IP address of outgoing TACACS+ packets default to the IP address of the egress interface.

**Mode** Global Configuration

**Usage notes** Setting the source interface ensures that all TACACS+ packets sent from the device will have the same source IP address. Once configured this affects all TACACS+ packets, namely accounting, authentication, and authorization.

If the specified interface is down or there is no IP address on the interface, then the source IP address of outgoing TACACS+ packets will default to the IP address of the egress interface.

**Example** To configure all outgoing TACACS+ packets to use the IP address of the loop-back "lo" interface as the source IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ip tacacs source-interface lo
```

To reset the source interface configuration for all TACACS+ packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip tacacs source-interface
```

**Related commands** [tacacs-server host](#)  
[show tacacs+](#)

**Command changes** Version 5.4.6-2.1: command added

# show tacacs+

**Overview** This command displays the current TACACS+ server configuration and status.

**Syntax** show tacacs+

**Mode** User Exec and Privileged Exec

**Example** To display the current status of TACACS+ servers, use the command:

```
awplus# show tacacs+
```

**Output** Figure 40-1: Example output from the **show tacacs+** command

|                              |                  |
|------------------------------|------------------|
| TACACS+ Global Configuration |                  |
| Source Interface             | : not configured |
| Timeout                      | : 5 sec          |
| Server Host/<br>IP Address   | Server<br>Status |
| -----                        |                  |
| 192.168.1.10                 | Alive            |
| 192.168.1.11                 | Unknown          |

**Table 1:** Parameters in the output of the **show tacacs+** command

| Output Parameter       | Meaning                                                                                 |
|------------------------|-----------------------------------------------------------------------------------------|
| Source Interface       | IP address of source interface if set with <a href="#">ip tacacs source-interface</a> . |
| Timeout                | A time interval in seconds.                                                             |
| Server Host/IP Address | TACACS+ server hostname or IP address.                                                  |
| Server Status          | The status of the authentication port.                                                  |
|                        | Alive      The server is alive.                                                         |
|                        | Dead      The server has timed out.                                                     |
|                        | Error      The server is not responding or there is an error in the key string entered. |
|                        | Unknown      The server is never used or the status is unknown.                         |
|                        | Unreachable      The server is unreachable.                                             |
|                        | Unresolved      The server name can not be resolved.                                    |

**Command changes** Version 5.4.6-2.1: **Source Interface** parameter added



# tacacs-server host

**Overview** Use this command to specify a remote TACACS+ server host for authentication, authorization and accounting, and to set the shared secret key to use with the TACACS+ server. The parameters specified with this command override the corresponding global parameters for TACACS+ servers.

Use the **no** variant of this command to remove the specified server host as a TACACS+ authentication and authorization server.

**Syntax** `tacacs-server host {<host-name>|<ip-address>} [key [8] <key-string>]`  
`no tacacs-server host {<host-name>|<ip-address>}`

| Parameter    | Description                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <host-name>  | Server host name. The DNS name of the TACACS+ server host.                                                                                                                                                                                                                                                                                                                                                                     |
| <ip-address> | The IP address of the TACACS+ server host, in dotted decimal notation A.B.C.D.                                                                                                                                                                                                                                                                                                                                                 |
| key          | Set shared secret key with TACACS+ servers.                                                                                                                                                                                                                                                                                                                                                                                    |
| 8            | Specifies that you are entering a password as a string that has already been encrypted instead of entering a plain text password. The running config displays the new password as an encrypted string even if password encryption is turned off.                                                                                                                                                                               |
| <key-string> | Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and the TACACS+ server. This key must match the encryption used on the TACACS+ server. This setting overrides the global setting of the <a href="#">tacacs-server key</a> command. If no key value is specified, the global value is used. |

**Default** No TACACS+ server is configured by default.

**Mode** Global Configuration

**Usage** A TACACS+ server host cannot be configured multiple times like a RADIUS server.

As many as four TACACS+ servers can be configured and consulted for login authentication, enable password authentication and accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, not if a login authentication attempt is rejected. The reasons a server would fail are:

- it is not network reachable
- it is not currently TACACS+ capable

- it cannot communicate with the switch properly due to the switch and the server having different secret keys

**Examples** To add the server tac1.company.com as the TACACS+ server host, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host tac1.company.com
```

To set the secret key to 'secret' on the TACACS+ server 192.168.1.1, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host 192.168.1.1 key secret
```

To remove the TACACS+ server tac1.company.com, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server host tac1.company.com
```

**Related commands**

- [aaa accounting commands](#)
- [aaa authentication login](#)
- [tacacs-server key](#)
- [tacacs-server timeout](#)
- [show tacacs+](#)

**Command changes** Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

# tacacs-server key

**Overview** This command sets a global secret key for TACACS+ authentication, authorization and accounting. The shared secret text string is used for TACACS+ communications between the switch and all TACACS+ servers.

Note that if no secret key is explicitly specified for a TACACS+ server with the [tacacs-server host](#) command, the global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to remove the global secret key.

**Syntax** `tacacs-server key [8] <key-string>`  
`no tacacs-server key`

| Parameter    | Description                                                                                                                                                                                                                                                                 |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8            | Specifies a string in an encrypted format instead of plain text. The running config will display the new password as an encrypted string even if password encryption is turned off.                                                                                         |
| <key-string> | Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and all TACACS+ servers. This key must match the encryption used on the TACACS+ server. |

**Mode** Global Configuration

**Usage notes** Use this command to set the global secret key shared between this client and its TACACS+ servers. If no secret key is specified for a particular TACACS+ server using the [tacacs-server host](#) command, this global key is used.

**Examples** To set the global secret key to `secret` for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server key secret
```

To delete the global secret key for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server key
```

**Related commands** [tacacs-server host](#)  
[show tacacs+](#)

# tacacs-server timeout

- Overview** Use this command to specify the TACACS+ global timeout value. The timeout value is how long the device waits for a reply to a TACACS+ request before considering the server to be dead.
- Note that this command configures the **timeout** parameter for TACACS+ servers globally.
- The **no** variant of this command resets the transmit timeout to the default (5 seconds).

**Syntax** `tacacs-server timeout <seconds>`  
`no tacacs-server timeout`

| Parameter | Description                                                |
|-----------|------------------------------------------------------------|
| <seconds> | TACACS+ server timeout in seconds, in the range 1 to 1000. |

**Default** The default timeout value is 5 seconds.

**Mode** Global Configuration

**Examples** To set the timeout value to 3 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server timeout 3
```

To reset the timeout period for TACACS+ servers to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server timeout
```

**Related commands** [tacacs-server host](#)  
[show tacacs+](#)

# Part 6: High Availability

# 41

# VRRP Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure the Virtual Router Redundancy Protocol (VRRP). For more information, see the [VRRP Feature Overview and Configuration Guide](#).

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Command List**
- [“advertisement-interval”](#) on page 1820
  - [“alternate-checksum-mode”](#) on page 1822
  - [“circuit-failover”](#) on page 1823
  - [“debug vrrp”](#) on page 1825
  - [“debug vrrp events”](#) on page 1826
  - [“debug vrrp packet”](#) on page 1827
  - [“disable \(VRRP\)”](#) on page 1828
  - [“enable \(VRRP\)”](#) on page 1829
  - [“preempt-mode”](#) on page 1830
  - [“priority”](#) on page 1832
  - [“router ipv6 vrrp \(interface\)”](#) on page 1834
  - [“router vrrp \(interface\)”](#) on page 1836
  - [“show debugging vrrp”](#) on page 1838
  - [“show running-config router ipv6 vrrp”](#) on page 1839
  - [“show running-config router vrrp”](#) on page 1840
  - [“show vrrp”](#) on page 1841
  - [“show vrrp counters”](#) on page 1843
  - [“show vrrp ipv6”](#) on page 1846

- [“show vrrp \(session\)”](#) on page 1847
- [“transition-mode”](#) on page 1848
- [“undebug vrrp”](#) on page 1850
- [“undebug vrrp events”](#) on page 1851
- [“undebug vrrp packet”](#) on page 1852
- [“virtual-ip”](#) on page 1853
- [“virtual-ipv6”](#) on page 1855
- [“vrrp vmac”](#) on page 1857

# advertisement-interval

**Overview** Use this command to configure the advertisement interval of the virtual router. This is the length of time, in seconds, between each advertisement sent from the master to its backup(s).

IPv6 VRRP advertisements are sent to the multicast address assigned to the VRRP group (ff02:0:0:0:0) and a backup virtual router has to join all multicast groups within this range. VRRP advertisements are sent to a multicast address (ff02::12) every second by default.

Use the **no** variant of this command to remove an advertisement interval of the virtual router, which has been set using the **advertisement-interval** command, and revert to the default advertisement interval of 1 second.

**Syntax** advertisement-interval [<1-255>|csec <1-4095>]  
no advertisement-interval

| Parameter | Description                                                         |
|-----------|---------------------------------------------------------------------|
| <1-255>   | Specifies the advertisement interval in seconds.                    |
| csec      | Use centiseconds instead of seconds for the advertisement interval. |
| <1-4095>  | Specifies the advertisement interval in centiseconds.               |

**Default** The default advertisement interval is 1 second.

**Mode** Router Configuration

**Usage notes** See the [VRRP Feature Overview and Configuration Guide](#) for more information about:

- setting the advertisement-interval when configuring VRRP
- using seconds for VRRPv2 host compatibility whenever you use [transition-mode](#) to upgrade or transition from VRRPv2 to VRRPv3
- VRRPv3 IPv4 configuration details
- VRRPv3 IPv6 configuration details

**Examples** The example below shows you how to configure the advertisement interval to 6 seconds for the VRRP IPv4 session with VR ID 5 on interface eth1:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# advertisement-interval 6
```



The example below shows you how to reset the advertisement interval to the default of 1 second for the VRRP IPv4 session with VR ID 5 on interface eth1:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# no advertisement-interval
```

The example below shows you how to configure the advertisement interval to 6 seconds for the VRRPv3 IPv6 session with VR ID 5 on interface eth1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 5 eth1
awplus(config-router)# advertisement-interval 6
```

**Related  
commands**

[router vrrp \(interface\)](#)  
[router ipv6 vrrp \(interface\)](#)

**Command  
changes**

Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# alternate-checksum-mode

**Overview** Use this command to enable an alternate checksum mode for VRRPv3 to allow inter-operability with some other vendors' products. The IPv4 checksum for VRRPv3 advertisements will then use a pseudo header in the calculation.

This mode may be required if the other product indicates checksum errors on VRRP packets sent by AlliedWare Plus devices.

Use the **no** variant of this command to disable the alternate checksum mode.

**Syntax** `alternate-checksum-mode`  
`no alternate-checksum-mode`

**Default** Disabled

**Mode** Router Configuration

**Example** To turn on the alternate checksum mode for VRRP instance 1 on interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 1 eth1
awplus(config-router)# alternate-checksum-mode
```

To turn off the alternate checksum mode for VRRP instance 1 on interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 1 eth1
awplus(config-router)# no alternate-checksum-mode
```

**Related commands** [show running-config](#)

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud  
Version 5.4.7-1.1: command added

# circuit-failover

**Overview** Use this command to enable the VRRP circuit failover feature.

Circuit failover enables the device to take action if the uplink interface goes down, so that the VRRP backup, whose uplink interface is still active, takes over as VRRP master. See the Usage section below and the [VRRP Feature Overview and Configuration Guide](#) for more information.

Use the **no** variant of this command to disable this feature.

**Syntax** `circuit-failover <interface> <1-253>`  
`no circuit-failover [<interface> <1-253>]`

| Parameter                      | Description                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;interface&gt;</code> | The interface of the router that is monitored. The interface must exist on the router, and is usually an upstream interface. Should the interface go down, then another router that is configured as a backup router in the group takes over as the master. You should configure the circuit failover on an interface other than the active VRRP interface - generally the uplink interface. |
| <code>&lt;1-253&gt;</code>     | Delta value. The value by which virtual routers decrement their priority value during a circuit failover event. Configure this value to be greater than the difference of priorities on the master and backup routers. In the case of failover, this priority delta value is subtracted from the current VR Master Router priority value.                                                    |

**Mode** Router Configuration

**Usage notes** You can use Circuit Failover to monitor up to 32 interfaces per VRRP instance. If a VRRP instance is configured to monitor multiple interfaces, the VRRP priority will be cumulatively decremented by the configured delta for each interface as it goes down.

For example, if VRRP is configured to monitor eth2 and eth3 with the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip address 192.168.1.1/24
awplus(config-if)# exit
awplus(config)# router vrrp 1 eth1
awplus(config-router)# virtual-ip 192.168.1.10 backup
awplus(config-router)# priority 100
awplus(config-router)# circuit-failover eth2 10
awplus(config-router)# circuit-failover eth3 20
```

then the following examples explain the effect of each eth interface going down:

- If only eth2 fails, then the VRRP priority will be decremented by 10. VRRP priority would be adjusted to become 90, because  $100 - 10 = 90$ .
- If only eth3 fails, then the VRRP priority will be decremented by 20. VRRP priority would be adjusted to become 80, because  $100 - 20 = 80$ .
- If both eth2 and eth3 fail, then the VRRP priority will be decremented by the cumulative delta values of all monitored interfaces. VRRP priority would therefore be adjusted to become 70, because  $100 - 10 - 20 = 70$ .

As each monitored interface recovers, the VRRP priority is incremented by the same delta value.

When you configure the delta values of the monitored interfaces, make sure their sum is high enough to ensure that the VRRP priority stays above zero if all the interfaces go down.

**Examples** To configure circuit failover on an IPv4 VRRP instance on interface eth2, so that if eth3 goes down, then the priority of VRRP instance 1 is reduced by 30, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 1 eth2
awplus(config-router)# circuit-failover eth3 30
```

To remove all configured circuit failovers for the VRRP IPv4 session with VR ID 1 on interface eth2, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 1 eth2
awplus(config-router)# no circuit-failover
```

To configure circuit failover on a VRRPv3 IPv6 session with VR ID 1 on interface eth2, so that when interface eth3 goes down, the priority of VRRP instance 1 is reduced by 30, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 1 eth2
awplus(config-router)# circuit-failover eth3 30
```

To remove all configured circuit failovers for the VRRPv3 IPv6 session with VR ID 1 on interface eth2, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 1 eth2
awplus(config-router)# no circuit-failover
```

**Related commands** [router vrrp \(interface\)](#)  
[router ipv6 vrrp \(interface\)](#)

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# debug vrrp

**Overview** Use this command to specify debugging options for VRRP. The **all** parameter turns on all the debugging options.

Use the **no** variant of this command to disable this function.

**Syntax** `debug vrrp [all]`  
`no debug vrrp [all]`

**Mode** Privileged Exec and Global Configuration

**Usage notes** See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 debugging details.

**Examples** The example below shows you how to enable all debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp all
```

The example below shows you how to disable all debugging for VRRP:

```
awplus# configure terminal
awplus(config)# no debug vrrp all
```

**Related commands** [show debugging vrrp](#)  
[undebug vrrp](#)

# debug vrrp events

**Overview** Use this command to specify debugging options for VRRP event troubleshooting.  
Use the **no** variant of this command to disable this function.

**Syntax** `debug vrrp events`  
`no debug vrrp events`

**Mode** Privileged Exec and Global Configuration

**Usage notes** The **debug vrrp events** command enables the display of debug information related to VRRP internal events.  
See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 debugging details.

**Examples** The example below shows you how to enable events debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp events
```

The example below shows you how to disable events debugging for VRRP:

```
awplus# configure terminal
awplus(config)# no debug vrrp events
```

**Related commands** [show debugging vrrp](#)  
[undebg vrrp events](#)

# debug vrrp packet

**Overview** Use this command to specify debugging options for VRRP packets.  
Use the **no** variant of this command to disable this function.

**Syntax** debug vrrp packet [send|recv]  
no debug vrrp packet [send|recv]

| Parameter | Description                                          |
|-----------|------------------------------------------------------|
| send      | Specifies the debug option set for sent packets.     |
| recv      | Specifies the debug option set for received packets. |

**Mode** Privileged Exec and Global Configuration

**Usage notes** The **debug vrrp packet** command enables the display of debug information related to the sending and receiving of packets.  
See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 debugging details.

**Examples** The example below shows you how to enable received and sent packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp packet
```

The example below shows you how to enable only received packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp packet recv
```

The example below shows you how to enable only sent packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp packet send
```

The example below shows you how to disable packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# no debug vrrp packet
```

**Related commands** [show debugging vrrp](#)  
[undebug vrrp packet](#)

# disable (VRRP)

**Overview** Use this command to disable a VRRP IPv4 session or a VRRPv3 IPv6 session on the router to stop it participating in virtual routing. Note that when this command is configured then a backup router assumes the role of master router depending on its priority. See the [enable \(VRRP\)](#) command to enable a VRRP IPv4 session or a VRRPv3 IPv6 session on the router.

**Syntax** `disable`

**Mode** Router Configuration

**Usage notes** See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv4 and IPv6 configuration details.

**Examples** The example below shows you how to disable the VRRP session for VRRP VR ID 5 on eth1:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# disable
```

The example below shows you how to disable the VRRPv3 session for VRRPv3 VR ID 3 on eth1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 eth1
awplus(config-router)# disable
```

**Related commands** [enable \(VRRP\)](#)  
[router vrrp \(interface\)](#)  
[router ipv6 vrrp \(interface\)](#)  
[show vrrp](#)

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud



# enable (VRRP)

**Overview** Use this command to enable the VRRP session on the router to make it participate in virtual routing. To make changes to the VRRP configuration, first disable the router from participating in virtual routing using the [disable \(VRRP\)](#) command.

**Syntax** enable

**Mode** Router Configuration

**Usage notes** You must configure the virtual IP address and define the interface for the VRRP session (using the [virtual-ip](#) or [virtual-ipv6](#) and the [router vrrp \(interface\)](#) or [router ipv6 vrrp \(interface\)](#) commands) before using this command.

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv4 and IPv6 configuration details.

**Examples** To enable the VRRP session for VRRP VR ID 5 on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# enable
```

To enable the VRRPv3 session for VRRPv3 VR ID 3 on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 eth1
awplus(config-router)# enable
```

**Related commands**

- [disable \(VRRP\)](#)
- [router vrrp \(interface\)](#)
- [router ipv6 vrrp \(interface\)](#)
- [show vrrp](#)
- [virtual-ip](#)
- [virtual-ipv6](#)

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# preempt-mode

**Overview** Use this command to configure preempt mode. If preempt-mode is set to **true**, then the highest priority backup will always be the master when the default master is unavailable.

If preempt-mode is set to **false**, then a higher priority backup will not preempt a lower priority backup who is acting as master.

If preempt-mode is set to **true**, an extra parameter is available called **delay-time**. If the delay-time parameter is used, a VRRP router with a higher priority will wait the configured length of time before it preempts the lower priority VRRP router to take over as master.

**Syntax** `preempt-mode {true|false}[delay-time <0-3600>]`

| Parameter  | Description                                                                                                                                                       |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| true       | Preemption is enabled.                                                                                                                                            |
| false      | Preemption is disabled.                                                                                                                                           |
| delay-time | Enable preempting but delay the preempt by the amount of seconds specified by the delay-time value. Note, a delay-time of 0 means delayed preempting is disabled. |

**Default** The default is **true**.

**Mode** Router Configuration

**Usage notes** When the master router fails, the backup routers come online in priority order—highest to lowest. Preempt mode means that a higher priority backup router will take over the master role from a lower priority backup. Preempt mode set to **true** allows a higher priority backup router to relieve a lower priority backup router.

By default, a preemptive scheme is enabled whereby a higher priority backup virtual router that becomes available takes over from the backup virtual router that was previously elected to become the master virtual router.

This preemptive scheme can be disabled using the **preempt-mode false** command. If preemption is disabled on a backup virtual router that is starting up, and this router has a higher priority than the current master, the higher priority backup will not preempt the current master, and the lower priority master will stay in the master role.

See the [VRRP Feature Overview and Configuration Guide](#) for more information about:

- VRRPv3 IPv4 configuration details
- VRRPv3 IPv6 configuration details
- preempt mode and preempt delay-time

**Examples** The example below shows you how to configure preempt-mode as true for VRRP VR ID 5 on eth1:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# preempt-mode true
```

The example below shows you how to configure preempt-mode as false for VRRP VR ID 5 on eth1:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# preempt-mode false
```

The example below shows you how to configure preempt-mode as true for VRRPv3 VR ID 3 on eth1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 eth1
awplus(config-router)# preempt-mode true
```

The example below shows you how to configure preempt-mode as false for VRRPv3 VR ID 3 on eth1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 eth1
awplus(config-router)# preempt-mode false
```

The example below shows you how to configure delay-time as 20 seconds for VRRPv3 VR ID 5 on eth1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 5 eth1
awplus(config-router)# preempt-mode true delay-time 20
```

**Related commands**

- [circuit-failover](#)
- [priority](#)
- [router vrrp \(interface\)](#)
- [router ipv6 vrrp \(interface\)](#)

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# priority

**Overview** Use this command to configure the VRRP router priority within the virtual router. The highest priority router is Master (unless [preempt-mode](#) is false).

Use the **no** variant of this command to remove the VRRP router priority within the virtual router, which has been set using the **priority** command.

**Syntax** `priority <1-255>`  
`no priority`

| Parameter                  | Description                                                                                                       |
|----------------------------|-------------------------------------------------------------------------------------------------------------------|
| <code>&lt;1-255&gt;</code> | The priority. For the master router, use 255 for this parameter; otherwise use any number from the range <1-254>. |

**Default** On a master router default priority is 255; on a backup router, default priority is 100.

**Mode** Router Configuration

**Usage notes** Priority determines the role that each VRRP router plays and what happens if the master virtual router fails. If a VRRP router owns the IP address of the virtual router and the IP address of the interface, then this VRRP router functions as the master virtual router.

Priority also determines whether a VRRP router functions as a backup virtual router and the order of ascendancy to becoming a master virtual router if the master virtual router fails. Configure the priority of each backup virtual router with a value of 1 through 254.

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv4 and IPv6 configuration details.

**Examples** The example below shows you how to configure 101 as the priority for VRRP VR ID 5 on eth1:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# priority 101
```

The example below shows you how to remove the priority configured for VRRP VR ID 5 on eth1:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# no priority
```

The example below shows you how to configure 101 as the priority for VRRPv3 VR ID 3 on eth1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 eth1
awplus(config-router)# priority 101
```

The example below shows you how to remove the configured priority for VRRPv3 VR ID 3 on eth1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 eth1
awplus(config-router)# no priority
```

**Related commands** [circuit-failover](#)  
[preempt-mode](#)

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# router ipv6 vrrp (interface)

**Overview** Use this command to configure VRRPv3 for IPv6 and define the interface that will participate in virtual routing to send and receive advertisement messages. This command allows you to enter the Router Configuration mode.

Use the **no** variant of this command to remove the VRRPv3 for IPv6 configuration. Disable the VRRP session before using the **no** variant of this command.

**Syntax** `router ipv6 vrrp <vrid> <interface>`  
`no router ipv6 vrrp <vrid> <interface>`

| Parameter   | Description                                                                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <vrid>      | <1-255> The ID of the virtual router VRRPv3 IPv6 session to create.                                                                                                                                    |
| <interface> | Specify the name of the interface that will participate in the virtual routing. The interface must exist on the router. The interface specified sends and receives VRRPv3 IPv6 advertisement messages. |

**Mode** Global Configuration

**Usage notes** Use the required <interface> placeholder to define the interface that will participate in virtual routing. This interface is used for two purposes - to send/receive advertisement messages and to forward on behalf of the virtual router when in master state.

**NOTE:** *Configuring a high number of instances may adversely affect the device's performance, depending on the device CPU, the other protocols it is running, and whether you set the advertisement interval to less than 1 second.*

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv6 configuration details.

**Examples** The example below shows you how to enable a VRRPv3 session with VR ID 3 on eth1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 eth1
awplus(config-router)# enable
```

The example below shows you how to disable a VRRPv3 session with VR ID 3 on eth1:

```
awplus(config-router)# disable
awplus(config-router)# exit
awplus(config)# no router ipv6 vrrp 3 eth1
```

**Related commands** [advertisement-interval](#)  
[circuit-failover](#)

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# router vrrp (interface)

**Overview** Use this command to configure VRRP IPv4 and define the interface that will participate in virtual routing to send and receive advertisement messages. This command allows you to enter the Router Configuration mode.

Use the **no** variant of this command to remove the VRRP IPv4 configuration. Disable the VRRP session before using the **no** variant of this command.

**Syntax** `router vrrp <vrid> <interface>`  
`no router vrrp <vrid> <interface>`

| Parameter   | Description                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <vrid>      | <1-255> The ID of the virtual router VRRP IPv4 session to create.                                                                                                                                    |
| <interface> | Specify the name of the interface that will participate in the virtual routing. The interface must exist on the router. The interface specified sends and receives VRRP IPv4 advertisement messages. |

**Mode** Global Configuration

**Usage notes** Use the required <interface> placeholder to define the interface that will participate in virtual routing. This interface is used for two purposes - to send/receive advertisement messages and to forward on behalf of the virtual router when in master state.

**NOTE:** *Configuring a high number of instances may adversely affect the device's performance, depending on the device CPU, the other protocols it is running, and whether you set the advertisement interval to less than 1 second.*

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv4 configuration details.

**Examples** To enable a VRRP session with VR ID 5 on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# enable
```

To disable a VRRP session with VR ID 5 on eth1, use the commands:

```
awplus(config-router)# disable
awplus(config-router)# exit
awplus(config)# no router vrrp 5 eth1
```



**Related commands**

- advertisement-interval
- circuit-failover
- disable (VRRP)
- enable (VRRP)

**Command changes**    Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# show debugging vrrp

**Overview** Use this command to display the set VRRP debugging option. Use the terminal monitor command to display output on the console otherwise debug output is in the log file.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 debugging details.

**Syntax** `show debugging vrrp`

**Mode** User Exec and Privileged Exec

**Example** The example below shows you how to display VRRP debugging:

```
awplus# show debugging vrrp
```

**Related commands**

- [debug vrrp](#)
- [debug vrrp events](#)
- [debug vrrp packet](#)

# show running-config router ipv6 vrrp

**Overview** Use this command to show the running configuration for VRRPv3 IPv6.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv6 configuration details.

**Syntax** show running-config router vrrp

**Mode** Privileged Exec, Global Configuration, Line Configuration, and Interface Configuration.

**Example** The example below shows you how to display the running configuration for VRRPv3 IPv6:

```
awplus# show running-config router ipv6 vrrp
```

**Output** Figure 41-1: Example output from the **show running-config router ipv6 vrrp** command

```
!
router ipv6 vrrp 3 eth1
 virtual-ip fe80::202:b3ff:fed5:983e master
 circuit-failover eth1 3
 advertisement-interval 6
 preempt-mode false
!
```

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# show running-config router vrrp

**Overview** Use this command to show the running configuration for VRRP IPv4.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv4 configuration details.

**Syntax** `show running-config router vrrp`

**Mode** Privileged Exec, Global Configuration, Line Configuration, and Interface Configuration.

**Example** The example below shows you how to display the running configuration for VRRP IPv4:

```
awplus# show running-config router vrrp
```

**Output** Figure 41-2: Example output from the **show running-config router vrrp** command

```
!
router vrrp 2 eth1
 circuit-failover eth1 2
 advertisement-interval 4
 preempt-mode true
!
```

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# show vrrp

- Overview** Use this command to display information about all VRRP IPv4 sessions. This command shows a summary when the optional **brief** parameter is used.
- For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).
- See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv4 configuration details.

**Syntax** `show vrrp [brief]`

| Parameter | Description                     |
|-----------|---------------------------------|
| brief     | Brief summary of VRRP sessions. |

**Mode** User Exec and Privileged Exec

**Example** To display information about all VRRP IPv4 sessions, enter the command:

```
awplus# show vrrp
```

To display brief summary output about VRRP IPv4 sessions, enter the command:

```
awplus# show vrrp brief
```

**Output** Figure 41-3: Example output from the **show vrrp** command

```
awplus#show vrrp
VMAC enabled
Address family IPv4
VRRP Id: 1 on interface: eth1
State: AdminUp - Master
Virtual IP address: 192.168.1.2 (Not-owner)
Priority is 100
Advertisement interval: 100 centiseconds
Preempt mode: TRUE
Multicast membership on IPv4 interface eth1: JOINED
Transition mode: FALSE
Accept mode: FALSE
Master address: 192.168.1.3
High
Availability: enabled
wan-bypass 1 (eth1) is on
```

Figure 41-4: Example output from the **show vrrp brief** command

```
awplus#show vrrp brief
```

| Interface | Grp | Prio | Own | Pre | State  | Master addr  | Group addr     |
|-----------|-----|------|-----|-----|--------|--------------|----------------|
| eth1      | 1   | 200  | N   | P   | Master | 192.168.10.4 | 192.168.10.253 |
| eth1      | 2   | 150  | N   | P   | Backup | 192.168.10.4 | 192.168.10.254 |
| eth2      | 3   | 200  | N   | P   | Master | 192.168.11.4 | 192.168.11.253 |
| eth2      | 4   | 150  | N   | P   | Backup | 192.168.11.4 | 192.168.11.254 |

**Related commands**    [enable \(VRRP\)](#)  
                          [disable \(VRRP\)](#)

**Command changes**    Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# show vrrp counters

**Overview** This command displays VRRP SNMP counters on the console, as described in the VRRP MIB and RFC2787, for debugging use while you configure VRRP with commands in this chapter.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show vrrp counters`

**Mode** User Exec and Privileged Exec

**Usage notes** The output has a section for global counters and a section of counters for each VRRP instance configured. See the descriptions of the counters below the sample output as per RFC2787.

**NOTE:** Note that the counters displayed with this commands are the same counters as described in RFC 2787, except for the “Monitored Circuit Up” and “Monitored Circuit Down” counters, which are additions beyond the MIB.

**Example** To display information about VRRP SNMP counters on the console, enter the command:

```
awplus# show vrrp counters
```

Figure 41-5: Example output from the **show vrrp counters** command

```
awplus#show vrrp counters
VRRP Global Counters:
Checksum Errors 230
Version Errors 0
VRID Errors 230

VRRP IPv4 counters for VR 10/eth1:
Master Transitions 0
Received Advertisements ... 0
Internal Errors 0
TTL Errors 0
Received Priority 0 Pkt ... 0
Sent Priority 0 Pkt 0
Received Invalid Type 0
Address List Errors 0
Packet Length Errors 0
Monitored Circuit Up 0
Monitored Circuit Down..... 0
```

```
VRRP IPv4 counters for VR 100/eth2:
Master Transitions 1
Received Advertisements ... 1614
Internal Errors 0
TTL Errors 0
Received Priority 0 Pkt ... 0
Sent Priority 0 Pkt 0
Received Invalid Type 0
Address List Errors 0
Packet Length Errors 0
Monitored Circuit Up 0
Monitored Circuit Down..... 2
```

**Table 1:** Global counters with descriptions for the **show vrrp counters** command:

| Counter         | Description                                                                              |
|-----------------|------------------------------------------------------------------------------------------|
| Checksum Errors | The total number of VRRP packets received with an invalid VRRP checksum value.           |
| Version Errors  | The total number of VRRP packets received with an unknown or unsupported version number. |
| VRID Errors     | The total number of VRRP packets received with an invalid VRID for this virtual router.  |

**Table 2:** Per VR counters with descriptions for the **show vrrp counters** command:

| Counter                 | Description                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Master Transitions      | The total number of times that this virtual router's state has transitioned to MASTER.                                                                          |
| Received Advertisements | The total number of VRRP advertisements received by this virtual router.                                                                                        |
| Internal Errors         | The total number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router. |
| TTL Errors              | The total number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.                                                    |
| Received Priority 0 Pkt | The total number of VRRP packets received by the virtual router with a priority of '0'.                                                                         |
| Sent Priority 0 Pkt     | The total number of VRRP packets sent by the virtual router with a priority of '0'.                                                                             |
| Received Invalid Type   | The number of VRRP packets received by the virtual router with an invalid value in the 'type' field.                                                            |
| Address List Errors     | The total number of packets received for which the address list does not match the locally configured list for the virtual router.                              |



**Table 2:** Per VR counters with descriptions for the **show vrrp counters** command: (cont.)

| Counter                | Description                                                                                        |
|------------------------|----------------------------------------------------------------------------------------------------|
| Packet Length Errors   | The total number of packets received with a packet length less than the length of the VRRP header. |
| Monitored Circuit Up   | The total number of times the monitored circuit has generated the UP event.                        |
| Monitored Circuit Down | The total number of times the monitored circuit has generated the down event.                      |

**Command changes**

Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# show vrrp ipv6

**Overview** Use this command to display information about all configured VRRPv3 IPv6 sessions for all interfaces, or all VRRPv3 IPv6 sessions for a given interface with the optional parameter.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv6 configuration details.

**Syntax** `show vrrp ipv6 [<interface>]`

| Parameter   | Description                                                                                                                                                                                            |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface> | Specify the name of the interface that will participate in the virtual routing. The interface must exist on the router. The interface specified sends and receives VRRPv3 IPv6 advertisement messages. |

**Mode** User Exec and Privileged Exec

**Example** To display information about all VRRPv3 IPv6 sessions, enter the command:

```
awplus# show vrrp ipv6
```

**Output** Figure 41-6: Example output from the **show vrrp ipv6** command for a specific interface

```
awplus#show vrrp ipv6 eth1
VrId <1>
State is Master
Virtual IP is fe80::202:b3ff:fed5:983e (Owner)
Interface is eth1
Priority is 255
Advertisement interval is 4 sec
Preempt mode is FALSE
```

**Related commands** [enable \(VRRP\)](#)  
[disable \(VRRP\)](#)

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# show vrrp (session)

**Overview** Use this command to display information for a particular VRRP session.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv4 configuration details.

**Syntax** `show vrrp <vrid> <interface>`

| Parameter   | Description                                                                                 |
|-------------|---------------------------------------------------------------------------------------------|
| <vrid>      | <1-255> The virtual router ID for which to display information. Session must already exist. |
| <interface> | The interface to display information about.                                                 |

**Mode** User Exec and Privileged Exec

**Example** To display information about VRRP session 1 configured on eth1, use the command:

```
awplus# show vrrp 1 eth1
```

**Output** Figure 41-7: Example output from the **show vrrp** command for a specific interface

```
awplus#show vrrp 1 eth2
Address family IPv4
VrId <1>
 Interface is eth1
 State is Initialize
 Virtual IP address is 10.10.11.250 (Not IP owner)
 Priority is 100
 Advertisement interval is 1 sec
 Preempt mode is TRUE
 Multicast membership on IPv4 interface eth1: JOINED
 Transition mode: FALSE
 Accept mode: TRUE
 Master address: 192.168.24.5
```

In this example, the output shows that a Virtual IP address has been set.

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# transition-mode

**Overview** Use this command to configure the IPv4 transition mode. Transition mode allows you to upgrade from VRRPv2 to VRRPv3 and gives interoperability between VRRPv2 and VRRPv3.

If transition-mode is set to **true**, then the IPv4 transition mode is enabled and VRRPv2 and VRRPv3 advertisements are sent allowing VRRPv2 and VRRPv3 interoperability. Received VRRPv2 advertisement packets are accepted and processed when transition-mode is true.

If transition-mode is set to **false**, then the IPv4 transition mode is disabled and only VRRPv3 advertisements are sent. Received VRRPv2 advertisement packets are dropped.

Note the [advertisement-interval](#) should not be configured to less than 1 second when using transition-mode. VRRPv2 can only use advertisements in whole second intervals.

**Syntax** `transition-mode {true|false}`

| Parameter | Description                                                                                                                                                                                           |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| true      | Transition mode is enabled. This results in VRRPv2 and VRRPv3 IPv4 advertisements being sent. Transition mode is only available on VRRPv3 for interoperability with VRRPv2 while upgrading to VRRPv3. |
| false     | Transition mode is disabled. This stops VRRPv2 IPv4 advertisements being sent. Only VRRPv3 advertisements are sent when disabled. Disable transition-mode after upgrading from VRRPv2 to VRRPv3.      |

**Default** The default is **false**.

**Mode** Router Configuration

**Usage notes** See the [VRRP Feature Overview and Configuration Guide](#) for more information about:

- VRRPv3 IPv4 configuration details
- VRRPv3 IPv6 configuration details
- configuring transition mode to upgrade from VRRPv2 to VRRPv3.

**Examples** The example below shows you how to configure IPv4 transition-mode as true for VRRP VR ID 5 on eth1:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# transition-mode true
```

The example below shows you how to configure IPv4 transition-mode as false for VRRP VR ID 5 on eth1:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# transition-mode false
```

**Related commands** [router vrrp \(interface\)](#)

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# undebg vrrp

**Overview** Use this command to disable all VRRP debugging.

**Syntax** undebg vrrp all

**Mode** Privileged Exec

**Example** The example below shows you how to disable all VRRP debugging:

```
awplus# undebg vrrp all
```

**Related commands** [debug vrrp](#)

# undebg vrrp events

**Overview** Use this command to disable debugging options for VRRP event troubleshooting.

**Syntax** undebg vrrp events

**Mode** Privileged Exec

**Example** The example below shows you how to disable VRRP event debugging:

```
awplus# undebg vrrp events
```

**Related commands** [debug vrrp events](#)

# undebg vrrp packet

**Overview** Use this command to disable debugging options for VRRP packets.

**Syntax** `undebg vrrp packet [send|recv]`

| Parameter | Description                                        |
|-----------|----------------------------------------------------|
| send      | Disable the debug option set for sent packets.     |
| recv      | Disable the debug option set for received packets. |

**Mode** Privileged Exec

**Examples** The example below shows you how to disable VRRP sent packet debugging:

```
awplus# undebg vrrp packet send
```

The example below shows you how to disable VRRP received packet debugging:

```
awplus# undebg vrrp packet recv
```

The example below shows you how to disable all VRRP packet debugging:

```
awplus# undebg vrrp packet
```

**Related commands** [debug vrrp packet](#)



# virtual-ip

**Overview** Use this command to set the virtual IP address for the VRRP session. This is the IP address of the virtual router that end hosts set as their default gateway.

Use the **no** variant of this command to disable this feature.

**Syntax** `virtual-ip <ip-address> [master|backup|owner]`  
`no virtual-ip`

| Parameter    | Description                                                                                                                                                                                                       |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-address> | The virtual IPv4 address of the virtual router, entered in dotted decimal format A.B.C.D.                                                                                                                         |
| master       | Sets the default state of the VRRP router within the Virtual Router as <b>master</b> . For master, the router must own the Virtual IP address. Specify the <b>owner</b> option before using <b>master</b> option. |
| backup       | Sets the default state of the VRRP router within the Virtual Router as <b>backup</b> .                                                                                                                            |
| owner        | Sets the IPv6 address of the VRRP router within the Virtual Router as the <b>owner</b> . Specify this before using the <b>master</b> option.                                                                      |

**Mode** Router Configuration

**Usage notes** The VRRP master and owner of the virtual IPv4 address for the VRRP session only responds to the packets destined to the virtual IPv4 address. The VRRP master that is not an owner of the virtual IPv4 address for the VRRP session does not respond to the packets destined to the virtual IPv4 address, but forwards packets with a VMAC as the destination address. See the [vrrp vmac](#) command to enable and disable this feature.

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv4 configuration details.

**Examples** The example below shows you how to set the virtual IP address for VRRP VR ID 5 and the router as the VRRP master:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# virtual-ip 192.0.2.30 master
```

The example below shows you how to set the virtual IPv4 address for VRRP VR ID 5 and the router as the VRRP backup:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# virtual-ip 192.0.2.30 backup
```

The example below shows you how to set the virtual IPv4 address for VRRP VR ID 5 and the router as owner of the virtual IPv4 address:

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# virtual-ip 192.0.2.30 owner
```

The example below shows you how to disable the virtual IPv4 address for VRRP VR ID 5

```
awplus# configure terminal
awplus(config)# router vrrp 5 eth1
awplus(config-router)# no virtual-ip
```

**Related  
commands**

[router vrrp \(interface\)](#)  
[enable \(VRRP\)](#)  
[vrrp vmac](#)

**Command  
changes**

Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

# virtual-ipv6

**Overview** Use this command to set the virtual IPv6 address for the VRRPv3 session. This is the IPv6 address of the virtual router that end hosts set as their default gateway.

Note that the primary IPv6 address specified is an IPv6 link-local address. See the Usage note below for further information.

Use the **no** variant of this command to disable this feature.

**Syntax** `virtual-ipv6 <ipv6-address> [master|backup]  
[primary|secondary]  
no virtual-ipv6`

| Parameter                         | Description                                                                                                                                                                                                                                          |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-address&gt;</code> | The IPv6 address of the virtual router, entered in hexadecimal, in the format X:X::X:X.                                                                                                                                                              |
| <code>master</code>               | Sets <b>master</b> to be the default state of the VRRPv3 router within the Virtual Router. For <b>master</b> , we recommend using a Virtual IP address that is not owned by any of the VRRP routers in the same grouping (that share the same VRID). |
| <code>backup</code>               | Sets <b>backup</b> to be the default state of the VRRPv3 router within the Virtual Router.                                                                                                                                                           |
| <code>primary</code>              | Sets the specified address as the primary IPv6 address. The primary address must be a link-local IPv6 address.                                                                                                                                       |
| <code>secondary</code>            | Sets the specified address as the secondary IPv6 address. Normally this would be a globally-routable IPv6 address. This enables you to specify a globally-routable address as the default gateway address for all the hosts on an interface.         |

**Mode** Router Configuration

**Usage notes** The virtual router will reply to ping, telnet, and SSH requests to the virtual IP address. The virtual router will reply even if it does not own the virtual IP address.

The AlliedWare Plus VRRPv3 implementation supports one IPv6 virtual link local address per virtual router ID. Note that in the command examples fe80::1 is an IPv6 link-local address. An IPv6 link-local address is used because IPv6 link-local addresses are used by IPv6 ND (Neighbor Discovery). A host's default route to a router points to the IPv6 link-local address, not a specific global IPv6 address for the router. For the host's traffic to switch over to a backup router, the IPv6 link-local address of the router is used by VRRPv3.

See the [VRRP Feature Overview and Configuration Guide](#) for more information about VRRPv3 IPv6 configuration details.

**Examples** The example below shows you how to set the virtual IPv6 address for VRRPv3 VR ID 3 and the router as the VRRPv3 master:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 eth1
awplus(config-router)# virtual-ipv6 fe80::1 master
```

The example below shows you how to set the virtual IPv6 address for VRRPv3 VR ID 3 and the router as the VRRPv3 backup:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 eth1
awplus(config-router)# virtual-ipv6 fe80::1 backup
```

The example below shows you disable the virtual IPv6 address for VRRPv3 VR ID 3:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 eth1
awplus(config-router)# no virtual-ipv6
```

**Related commands**

- [router ipv6 vrrp \(interface\)](#)
- [enable \(VRRP\)](#)
- [vrrp vmac](#)

**Command changes** Version 5.5.2-2.1: command added on 10GbE UTM Firewall and AR4000S-Cloud

## vrrp vmac

**Overview** Use this command to enable or disable the VRRP Virtual MAC feature. This feature is used by VRRP to make the hosts use the virtual MAC address as the physical hardware address of their gateway.

A VRRP router master will use the virtual MAC address for any ARP responses associated with the virtual IP address, or any gratuitous ARPs sent on behalf of the virtual IP address.

All VRRP advertisements are sent using this virtual MAC address as the source MAC address.

The virtual MAC address has the form 00:00:5e:00:01:<VRID>, where VRID is the ID of the Virtual Router.

**Syntax** `vrrp vmac {enable|disable}`

**Mode** Global Configuration

**Examples** To enable Virtual MAC enter:

```
awplus# configure terminal
awplus(config)# vrrp vmac enable
```

To disable Virtual MAC enter:

```
awplus# configure terminal
awplus(config)# vrrp vmac disable
```

**Related commands** [virtual-ip](#)  
[virtual-ipv6](#)

# Part 7: Network Management

# 42

# AMF and AMF Plus Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for AMF and AMF Plus commands. AMF is the Allied Telesis Autonomous Management Framework™, and AMF Plus is an expanded version of AMF. Both AMF and AMF Plus are a suite of features that combine to simplify network management across all supported network equipment from the core to the edge. They also integrate with Vista Manager, our graphical monitoring and management platform.

On the AlliedWare Plus command line, AMF and AMF Plus are identical. The difference between them is in Vista Manager, where AMF Plus includes additional AMF Plus intent-based networking features.

**In the rest of this chapter, we use 'AMF' to refer to both AMF and AMF Plus.**

**AMF master nodes** Every AMF network must have at least one master node, which acts as the core of the AMF network. Not all AlliedWare Plus devices are capable of acting as a AMF master. See the [AMF Feature Overview and Configuration Guide](#) for information about master support.

**AMF edge** AlliedWare Plus CentreCOM® Series switches can only be used as edge switches in an AMF network. The full management power and convenience of AMF is available on these switches, but they can only link to one other AMF node. They cannot form cross-links or virtual links.

**AMF naming convention** When AMF is enabled on a device, it will automatically be assigned a host name. If a host name has already been assigned, by using the command [hostname](#) on page 255, this will remain. If however, no host name has been assigned, then the name applied will be the prefix, **host\_** followed (without a space) by the MAC address of the device. For example, a device whose MAC address is **0016.76b1.7a5e** will have the name **host\_0016\_76b1\_7a5e** assigned to it.

To efficiently manage your network using AMF, we strongly advise that you devise a naming convention for your network devices, and apply an appropriate hostname to each device in your AMF network.

**AMF and STP** On AR-Series UTM firewalls and Secure VPN routers, you cannot use STP at the same time as AMF.

- Command List**
- ["application-proxy ip-filter"](#) on page 1865
  - ["application-proxy quarantine-vlan"](#) on page 1866
  - ["application-proxy redirect-url"](#) on page 1867
  - ["application-proxy threat-protection"](#) on page 1868
  - ["application-proxy threat-protection send-summary"](#) on page 1870
  - ["application-proxy whitelist advertised-address"](#) on page 1871
  - ["application-proxy whitelist enable"](#) on page 1872
  - ["application-proxy whitelist protection tls"](#) on page 1873
  - ["application-proxy whitelist server"](#) on page 1874
  - ["application-proxy whitelist trustpoint \(deprecated\)"](#) on page 1876
  - ["area-link"](#) on page 1877
  - ["atmf-arealink"](#) on page 1879
  - ["atmf-link"](#) on page 1881
  - ["atmf amfplus-license-only"](#) on page 1882
  - ["atmf area"](#) on page 1884
  - ["atmf area password"](#) on page 1886
  - ["atmf authorize"](#) on page 1888
  - ["atmf authorize provision"](#) on page 1890
  - ["atmf backup"](#) on page 1892
  - ["atmf backup area-masters delete"](#) on page 1893
  - ["atmf backup area-masters enable"](#) on page 1894
  - ["atmf backup area-masters now"](#) on page 1895
  - ["atmf backup area-masters synchronize"](#) on page 1896
  - ["atmf backup bandwidth"](#) on page 1897
  - ["atmf backup delete"](#) on page 1898
  - ["atmf backup enable"](#) on page 1899
  - ["atmf backup guests delete"](#) on page 1900
  - ["atmf backup guests enable"](#) on page 1901
  - ["atmf backup guests now"](#) on page 1902
  - ["atmf backup guests synchronize"](#) on page 1903
  - ["atmf backup now"](#) on page 1904
  - ["atmf backup redundancy enable"](#) on page 1906
  - ["atmf backup server"](#) on page 1907



- [“atmf backup stop”](#) on page 1909
- [“atmf backup synchronize”](#) on page 1910
- [“atmf cleanup”](#) on page 1911
- [“atmf container”](#) on page 1912
- [“atmf container login”](#) on page 1913
- [“atmf controller”](#) on page 1914
- [“atmf distribute firmware”](#) on page 1915
- [“atmf domain vlan”](#) on page 1917
- [“atmf enable”](#) on page 1920
- [“atmf group \(membership\)”](#) on page 1921
- [“atmf guest-class”](#) on page 1923
- [“atmf log-verbose”](#) on page 1925
- [“atmf management subnet”](#) on page 1926
- [“atmf management vlan”](#) on page 1929
- [“atmf master”](#) on page 1931
- [“atmf mtu”](#) on page 1932
- [“atmf network-name”](#) on page 1933
- [“atmf provision \(interface\)”](#) on page 1934
- [“atmf provision node”](#) on page 1935
- [“atmf reboot-rolling”](#) on page 1937
- [“atmf recover”](#) on page 1941
- [“atmf recover guest”](#) on page 1943
- [“atmf recover led-off”](#) on page 1944
- [“atmf recover over-eth”](#) on page 1945
- [“atmf recovery-server”](#) on page 1946
- [“atmf remote-login”](#) on page 1948
- [“atmf restricted-login”](#) on page 1950
- [“atmf retry guest-link”](#) on page 1952
- [“atmf secure-mode”](#) on page 1953
- [“atmf secure-mode certificate expire”](#) on page 1955
- [“atmf secure-mode certificate expiry”](#) on page 1956
- [“atmf secure-mode certificate renew”](#) on page 1957
- [“atmf secure-mode enable-all”](#) on page 1958
- [“atmf select-area”](#) on page 1960
- [“atmf topology-gui enable”](#) on page 1961

- [“atmf trustpoint”](#) on page 1962
- [“atmf virtual-crosslink”](#) on page 1964
- [“atmf virtual-link”](#) on page 1966
- [“atmf virtual-link description”](#) on page 1969
- [“atmf virtual-link protection”](#) on page 1970
- [“atmf working-set”](#) on page 1972
- [“bridge-group \(amf-container\)”](#) on page 1974
- [“clear application-proxy threat-protection”](#) on page 1976
- [“clear atmf links”](#) on page 1977
- [“clear atmf links virtual”](#) on page 1978
- [“clear atmf links statistics”](#) on page 1979
- [“clear atmf recovery-file”](#) on page 1980
- [“clear atmf secure-mode certificates”](#) on page 1981
- [“clear atmf secure-mode statistics”](#) on page 1982
- [“clone \(amf-provision\)”](#) on page 1983
- [“configure boot config \(amf-provision\)”](#) on page 1985
- [“configure boot system \(amf-provision\)”](#) on page 1987
- [“copy \(amf-provision\)”](#) on page 1989
- [“create \(amf-provision\)”](#) on page 1990
- [“debug atmf”](#) on page 1992
- [“debug atmf packet”](#) on page 1994
- [“delete \(amf-provision\)”](#) on page 1997
- [“discovery”](#) on page 1999
- [“description \(amf-container\)”](#) on page 2001
- [“erase factory-default”](#) on page 2002
- [“firmware-url”](#) on page 2003
- [“http-enable”](#) on page 2005
- [“identity \(amf-provision\)”](#) on page 2007
- [“license-cert \(amf-provision\)”](#) on page 2009
- [“locate \(amf-provision\)”](#) on page 2011
- [“log event-host”](#) on page 2013
- [“login-fallback enable”](#) on page 2014
- [“modeltype”](#) on page 2015
- [“service atmf-application-proxy”](#) on page 2016
- [“show application-proxy threat-protection”](#) on page 2017

- [“show application-proxy whitelist advertised-address”](#) on page 2019
- [“show application-proxy whitelist interface”](#) on page 2020
- [“show application-proxy whitelist server”](#) on page 2022
- [“show application-proxy whitelist supplicant”](#) on page 2023
- [“show atmf”](#) on page 2025
- [“show atmf area”](#) on page 2029
- [“show atmf area guests”](#) on page 2032
- [“show atmf area guests-detail”](#) on page 2034
- [“show atmf area nodes”](#) on page 2036
- [“show atmf area nodes-detail”](#) on page 2038
- [“show atmf area summary”](#) on page 2040
- [“show atmf authorization”](#) on page 2041
- [“show atmf backup”](#) on page 2044
- [“show atmf backup area”](#) on page 2048
- [“show atmf backup guest”](#) on page 2050
- [“show atmf container”](#) on page 2052
- [“show atmf detail”](#) on page 2055
- [“show atmf group”](#) on page 2057
- [“show atmf group members”](#) on page 2059
- [“show atmf guests”](#) on page 2061
- [“show atmf guests detail”](#) on page 2063
- [“show atmf links”](#) on page 2066
- [“show atmf links detail”](#) on page 2068
- [“show atmf links guest”](#) on page 2077
- [“show atmf links guest detail”](#) on page 2079
- [“show atmf links statistics”](#) on page 2083
- [“show atmf nodes”](#) on page 2086
- [“show atmf provision nodes”](#) on page 2088
- [“show atmf recovery-file”](#) on page 2090
- [“show atmf secure-mode”](#) on page 2091
- [“show atmf secure-mode audit”](#) on page 2093
- [“show atmf secure-mode audit link”](#) on page 2094
- [“show atmf secure-mode certificates”](#) on page 2095
- [“show atmf secure-mode sa”](#) on page 2098
- [“show atmf secure-mode statistics”](#) on page 2101

- ["show atmf tech"](#) on page 2103
- ["show atmf virtual-links"](#) on page 2106
- ["show atmf working-set"](#) on page 2108
- ["show debugging atmf"](#) on page 2109
- ["show debugging atmf packet"](#) on page 2110
- ["show running-config atmf"](#) on page 2111
- ["state"](#) on page 2112
- ["switchport atmf-agentlink"](#) on page 2114
- ["switchport atmf-arealink"](#) on page 2115
- ["switchport atmf-crosslink"](#) on page 2117
- ["switchport atmf-guestlink"](#) on page 2119
- ["switchport atmf-link"](#) on page 2121
- ["type atmf guest"](#) on page 2122
- ["type atmf node"](#) on page 2123
- ["undebbug atmf"](#) on page 2125
- ["username \(atmf-guest\)"](#) on page 2126

# application-proxy ip-filter

**Overview** Use this command to enable global IP filtering on a device. Once enabled the device will add a global ACL in response to a threat message from an AMF Security (AMF-Sec) Controller.

Use the **no** variant of this command to disable global IP filtering.

**Syntax** `application-proxy ip-filter`  
`no application-proxy ip-filter`

**Default** Global IP filtering is disabled by default.

**Mode** Global Configuration

**Usage notes** For this feature to work, the AMF Application Proxy service needs to be enabled on your network, using the command [service atmf-application-proxy](#).

**Example** To enable global IP filtering, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy ip-filter
```

To disable global IP filtering, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy ip-filter
```

**Related commands** [application-proxy redirect-url](#)  
[application-proxy threat-protection](#)  
[clear application-proxy threat-protection](#)  
[service atmf-application-proxy](#)  
[show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.5: command added

# application-proxy quarantine-vlan

**Overview** Use this command to set the quarantine VLAN to use when an AMF Security (AMF-Sec) Controller detects a threat. The port/s on which the threat is detected are moved to this VLAN if the [application-proxy threat-protection](#) action is set to **quarantine**.

Use the **no** variant of this command to delete the quarantine VLAN. If no quarantine VLAN is specified then no quarantine action will be performed.

**Syntax** `application-proxy quarantine-vlan <vlan-id>`  
`no application-proxy quarantine-vlan`

| Parameter                    | Description                                     |
|------------------------------|-------------------------------------------------|
| <code>&lt;vlan-id&gt;</code> | The ID of the VLAN to use. In the range 1-4094. |

**Default** By default, no quarantine VLAN is configured.

**Mode** Global Configuration

**Example** To configure VLAN 100 as the quarantine VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy quarantine-vlan 100
```

To delete the quarantine VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy quarantine-vlan
```

**Related commands** [application-proxy threat-protection](#)  
[clear application-proxy threat-protection](#)  
[application-proxy threat-protection send-summary](#)  
[service atmf-application-proxy](#)  
[show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.2: command added

# application-proxy redirect-url

**Overview** Use this command to redirect a user to a helpful URL when they are blocked because of an [application-proxy ip-filter](#).

Use the **no** variant of this command to remove the URL redirect.

**Syntax** `application-proxy redirect-url <url>`  
`no application-proxy redirect-url`

| Parameter                | Description                  |
|--------------------------|------------------------------|
| <code>&lt;url&gt;</code> | URL to redirect the user to. |

**Default** No URL is configured by default.

**Mode** Global Configuration

**Example** To configure a redirect URL, use the command:

```
awplus# application-proxy redirect-url http://my.dom/help.html
```

To remove a redirect URL, use the command:

```
awplus# no application-proxy redirect-url
```

**Related commands** [application-proxy ip-filter](#)  
[application-proxy threat-protection](#)  
[clear application-proxy threat-protection](#)  
[service atmf-application-proxy](#)  
[show application-proxy threat-protection](#)

**Command changes** Version 5.4.9-0.1: command added

# application-proxy threat-protection

**Overview** Use this command to set the blocking action to take when a threat detected message is received from an AMF Security (AMF-Sec) Controller.

Use the **no** variant of this command to disable threat protection blocking actions on the port.

**Syntax** `application-proxy threat-protection`  
`{drop|link-down|quarantine|log-only}`  
`no application-proxy threat-protection`

| Parameter  | Description                                                                                                                                                                      |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| drop       | Drop the traffic that generates the threat reports. This is a Layer 2 drop. Note that the device will only drop packets that arrive at the port, not packets sent from the port. |
| link-down  | Take the link down in response to threats, by setting it to error disabled.                                                                                                      |
| quarantine | Move the offending port to a quarantine VLAN.                                                                                                                                    |
| log-only   | Log when a threat is detected.                                                                                                                                                   |

**Default** Threat protection is disabled by default.

**Mode** Interface Configuration

**Example** To set the threat protection blocking action on port1.0.4 to drop, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# application-proxy threat-protection drop
```

To disable threat protection blocking actions on port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no application-proxy threat-protection
```

**Related commands**

- [application-proxy quarantine-vlan](#)
- [application-proxy threat-protection send-summary](#)
- [clear application-proxy threat-protection](#)
- [service atmf-application-proxy](#)
- [show application-proxy threat-protection](#)



**Command changes**

- Version 5.5.2-0.1: added to switch ports on AR series devices
- Version 5.4.9-0.1: **log-only** parameter added
- Version 5.4.7-2.2: command added

# application-proxy threat-protection send-summary

**Overview** Use this command to send a summary of all current threat-protection blocking requests to all AMF Application Proxy service nodes. This command can only be performed on an AMF master.

**Syntax** `application-proxy threat-protection send-summary`

**Mode** Privileged Exec

**Example** To send a summary of all current threat-protection blocking requests to all AMF Application Proxy service nodes, use the command:

```
awplus# application-proxy threat-protection send-summary
```

**Related commands**

- [application-proxy quarantine-vlan](#)
- [application-proxy threat-protection](#)
- [clear application-proxy threat-protection](#)
- [service atmf-application-proxy](#)
- [show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.2: command added

# application-proxy whitelist advertised-address

**Overview** Use this command to register a Layer 3 interface, and the IPv4 address that is attached to this interface, as the advertised application-proxy whitelist address for a device.

Use the **no** variant of this command to stop advertising the Layer 3 interface and its associated IPv4 address.

**Syntax** `application-proxy whitelist advertised-address <interface>`  
`no application-proxy whitelist advertised-address`

| Parameter                      | Description                                               |
|--------------------------------|-----------------------------------------------------------|
| <code>&lt;interface&gt;</code> | Layer 3 interface to configure as the advertised address. |

**Default** No address advertised by default.

**Mode** Global Configuration

**Example** To configure the IPv4 address attached to VLAN 1 as the advertised address, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist advertised-address
vlan1
```

To remove the advertised address, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy whitelist
advertised-address
```

**Related commands** [application-proxy whitelist server](#)  
[show application-proxy whitelist advertised-address](#)

**Command changes** Version 5.4.9-1.1: command added

# application-proxy whitelist enable

**Overview** Use this command to enable application-proxy whitelist based authentication on an interface.

Use the **no** variant of this command to disable the whitelist authentication.

**Syntax** `application-proxy whitelist enable`  
`no application-proxy whitelist enable`

**Default** Application-proxy whitelist is disabled by default.

**Mode** Interface Configuration

**Usage notes** When **port-control** is set to **auto**, the 802.1X authentication feature is executed on the interface, but only if the **aaa authentication dot1x** command has been issued.

If you attempt to change the authentication configuration on an interface that has threat protection quarantine configured, you will see the following error message:

```
% portx.x.x: Application Proxy quarantine configuration must be removed before port authentication is changed
```

Before changing the interface's authentication configuration you must either:

- remove the interface's threat protection configuration, or
- shut down the interface.

**Example** To enable application-proxy whitelist authentication on the interface port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# application-proxy whitelist enable
```

To disable application-proxy whitelist authentication on the interface port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no application-proxy whitelist enable
```

**Related commands**

- [application-proxy whitelist server](#)
- [show application-proxy whitelist interface](#)
- [show application-proxy whitelist server](#)
- [show application-proxy whitelist supplicant](#)

**Command changes** Version 5.4.9-0.1: command added

# application-proxy whitelist protection tls

**Overview** Use this command to configure the application-proxy whitelist control channel to use TLS protection. If no trustpoint is specified then TLS will operate without authentication.

Use the **no** variant of this command to stop using TLS.

**Syntax** `application-proxy whitelist protection tls [trustpoint <name>]`  
`no application-proxy whitelist protection tls`

| Parameter  | Description                                                                                                 |
|------------|-------------------------------------------------------------------------------------------------------------|
| trustpoint | Specify an optional trustpoint. If no trustpoint is specified then TLS will operate without authentication. |
| <name>     | Name of the trustpoint.                                                                                     |

**Default** TLS is disabled by default.

**Mode** Global Configuration

**Example** To configure an AMF application-proxy whitelist to use TLS with the trustpoint 'corpca', use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist protection tls
trustpoint corpca
```

To configure an AMF application-proxy whitelist to stop using TLS, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy whitelist protection tls
```

**Related commands** [application-proxy whitelist enable](#)  
[application-proxy whitelist server](#)  
[show application-proxy whitelist server](#)

**Command changes** Version 5.5.0-2.1: command added

# application-proxy whitelist server

**Overview** Use this command to set an AMF master to act as a whitelist authentication proxy between AMF members, acting as Network Access Servers, and an external whitelist RADIUS server.

Use the **no** variant of this command to disable the whitelist proxy functionality.

**Syntax** `application-proxy whitelist server <ip-address> key <key>  
[auth-port <1-65535>]`  
`no application-proxy whitelist server`

| Parameter                              | Description                                                                                            |
|----------------------------------------|--------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code>        | IPv4 address of the upstream RADIUS server in dotted decimal format A.B.C.D.                           |
| <code>key &lt;key&gt;</code>           | Set the shared secret encryption key for communication with the upstream RADIUS server.                |
| <code>auth-port &lt;1-65535&gt;</code> | Set the RADIUS server UDP port. This is only necessary if you don't want to use the default port 1812. |

**Default** Disabled by default.

**Mode** Global Configuration

**Example** To configure an AMF master to work as a proxy to the external RADIUS server 192.168.1.10, with shared secret 'mysecurekey', on port 1822, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist server 192.168.1.10
key mysecurekey auth-port 1822
```

To configure an AMF master to work as a proxy to the external RADIUS server 192.168.1.10, with shared secret 'mysecurekey', on the default port (1812), use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist server 192.168.1.10
key mysecurekey
```

To disable the whitelist proxy, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy whitelist server
```

**Related commands**

- [application-proxy whitelist enable](#)
- [service atmf-application-proxy](#)
- [show application-proxy whitelist interface](#)
- [show application-proxy whitelist server](#)

show application-proxy whitelist supplicant

**Command changes**    Version 5.4.9-0.1: command added

# application-proxy whitelist trustpoint (deprecated)

**Overview** This command has been deprecated. It has been replaced by the [application-proxy whitelist protection tls](#) command.

This command sets the trustpoint to use when communicating with the external whitelist RADIUS server. This enables RADIUS over TLS (RadSec) protection.

**Syntax** `application-proxy whitelist trustpoint <name>`  
`no application-proxy whitelist trustpoint`

**Command changes** Version 5.4.9-1.1: command added  
Version 5.5.0-2.1: command deprecated



# area-link

**Overview** Use this command to create an area-link between a Virtual AMF Appliance (VAA) host controller and an AMF container.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove an area-link from a container.

**Syntax** `area-link <area-name>`  
`no area-link`

| Parameter                      | Description                            |
|--------------------------------|----------------------------------------|
| <code>&lt;area-name&gt;</code> | AMF area name of the container's area. |

**Mode** AMF Container Configuration

**Usage notes** The AMF area-link connects the AMF controller on a VAA host to the AMF container. Once a container has been created with the [atmf container](#) command and an area-link configured with the **area-link** command, it can be enabled using the [state](#) command.

You can only configure a single area-link on a container. You will see the following message if you try and configure a second one:

```
% AreaLink already configured for this container
```

Each container has two virtual interfaces:

- Interface eth0, used to connect to the AMF controller on the VAA host via an AMF area-link, configured using this area-link command.
- Interface eth1, used to connect to the outside world using a bridged L2 network link, configured using the [bridge-group \(amf-container\)](#) command.

See the [AMF Feature Overview and Configuration\\_Guide](#) for more information on these virtual interfaces and links.

**Example** To create the area-link to "wlg" on container "vac-wlg-1", use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# area-link wlg
```

To remove an area-link from container “vac-wlg-1”, use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# no area-link
```

**Related  
commands**

[atmf container](#)  
[show atmf container](#)

**Command  
changes**

Version 5.4.7-0.1: command added

# atmf-arealink

**Overview** This command to enable an Eth interface, on an AR-series device, as an AMF area link. AMF area links are designed to operate between two nodes in different areas in an AMF network. This command is only available if your network is running in AMF secure mode (see [atmf secure-mode](#) for more information on AMF secure mode).

Use the **no** variant of this command to remove any AMF area links that may exist for the selected Eth interface.

**Syntax** `atmf-arealink remote-area <area-name> vlan <2-4094>`  
`no atmf-arealink`

| Parameter   | Description                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <area-name> | The name of the remote area that the interface is connecting to.                                                                     |
| <2-4094>    | The VLAN ID for the link. This VLAN cannot be used for any other purpose, and the same VLAN ID must be used at each end of the link. |

**Default** By default, no area links are configured

**Mode** Eth interface on an AR-series device.

**Usage notes** Run this command on the interface at both ends of the link.  
Each area must have the area-name configured, and the same area password must exist on both ends of the link.

Running this command will synchronize the area information stored on the two nodes.

You can configure multiple area links between two area nodes, but only one area link at any time will be in use. All other area links will block information, to prevent network storms.

**NOTE:** See the [switchport atmf-arealink](#) command to configure an AMF area link on an a switch port or link aggregator

**Example** To configure eth1 as an AMF area link to the 'Auckland' area on VLAN 6, use the following commands:

```
master_1# configure terminal
master_1(config)# interface eth1
master_1(config-if)# atmf-arealink remote-area Auckland vlan 6
```

To remove eth1 as an AMF area link, use the following commands:

```
master_1# configure terminal
master_1(config)# interface eth1
master_1(config-if)# no atmf-arealink
```

|                         |                                    |
|-------------------------|------------------------------------|
| <b>Related commands</b> | <a href="#">atmf area</a>          |
|                         | <a href="#">atmf area password</a> |
|                         | <a href="#">atmf virtual-link</a>  |
|                         | <a href="#">show atmf links</a>    |
| <b>Command changes</b>  | Version 5.5.0-1.1: command added   |

# atmf-link

**Overview** Use this command to enable an Eth interface on an AR-series device as an up/down AMF link. This command is only available if your network is running in AMF secure mode (see [atmf secure-mode](#) for more information on AMF secure mode).

Use the **no** variant of this command to remove any AMF link that may exist for the selected Eth interface.

**Syntax** atmf-link  
no atmf-link

**Mode** Eth interface on an AR-series device.

**Usage notes** Up/down links and virtual links interconnect domains in a vertical hierarchy, with the highest domain being the core domain. In effect, they form a tree of interconnected AMF domains. This tree must be loop-free. Therefore you must configure your up/down and virtual links so that no loops are formed.

If you run the command and AMF secure mode is not enabled, you will see the following error message:

```
Node_1(config)#int eth1
Node_1(config-if)#atmf-link
% Cannot configure eth1 because atmf secure-mode is not enabled.
```

**NOTE:** See the [switchport atmf-link](#) command to configure an AMF up/down link on an a switch port or link aggregator

**Example** To configure eth1 as an AMF up/down link, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface eth1
Node_1(config-if)# atmf-link
```

To remove eth1 as an AMF up/down link, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface eth1
Node_1(config-if)# no atmf-link
```

**Related commands** [atmf recover over-eth](#)  
[atmf secure-mode](#)  
[show atmf detail](#)  
[show atmf links](#)  
[switchport atmf-link](#)

**Command changes** Version 5.5.0-1.1: command added

# atmf amfplus-license-only

**Overview** Use this command if you want to use the AMF Plus features in Vista Manager EX, and you have a mixture of AMF and AMF Plus licenses on your master node. This command sets the AMF network to only count **AMF Plus** licensed nodes.

Use the **no** variant of this command to include both AMF and AMF Plus licenses when calculating the number of licensed nodes in an area count.

**Syntax** `atmf amfplus-license-only`  
`no atmf amfplus-license-only`

**Default** The **no** version is the default. That is, consider both AMF and AMF Plus licenses when calculating the number of licensed nodes.

**Mode** Global Configuration

**Usage notes** From software version 5.5.2-2.3 onwards, AMF licenses are no longer available to purchase. Instead, AMF Plus licenses become available. Existing AMF licenses remain valid. You only need to change to AMF Plus licenses if you want to manage more nodes, or use the new AMF Plus menu in Vista Manager.

**CAUTION:** *If the network has more AMF nodes than are licensed with AMF Plus:*

- AMF Plus will still be enabled in Vista Manager EX (provided there is no AMF license)
- any AMF nodes above the license count won't join the AMF network.

The AMF Plus menu replaces the AOI menu in Vista Manager EX when all the AMF Masters and Controllers have:

- An AMF Plus Controller/Master license on all Masters and Controllers, and
- No AMF Controller/Master licenses applied, or AMF Controller/Master licenses disabled with this command.

**Example** To set the AMF network to only count AMF Plus licensed nodes, use the commands:

```
awplus#configure terminal
awplus(config)#atmf amfplus-license-only
```

**Output** Figure 42-1: Example using **atmf amfplus-license-only**

```
ATMF Summary Information:
ATMF Status : Enabled
Network Name : gtnet
Node Name : node2
Role : Master
Restricted login : Enabled
Secure Mode : Disabled
Current ATMF Guests : 0
Current ATMF Nodes : 10
Total number of licensed nodes available is 22

node2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
node2(config)#atmf amfplus-license-only
node2(config)#15:41:36 node2 ATMF[1041]: The number of nodes
allowed on this ATMF network is 12

node2(config)#do show atmf
ATMF Summary Information:

ATMF Status : Enabled
Network Name : gtnet
Node Name : node2
Role : Master
Restricted login : Enabled
Secure Mode : Disabled
Current ATMF Guests : 0
Current ATMF Nodes : 10
Master is configured to allow only AMFPLUS Licenses
Total number of licensed nodes available is 12
```

**Related commands** [show atmf](#)

**Command changes** Version 5.5.3-0.1: command added

# atmf area

**Overview** This command creates an AMF area and gives it a name and ID number.

Use the **no** variant of this command to remove the AMF area.

This command is only valid on AMF controllers, master nodes and gateway nodes.

**Syntax** `atmf area <area-name> id <1-4094> [local]`  
`no atmf area <area-name>`

| Parameter   | Description                                                                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <area-name> | The AMF area name. The area name can be up to 15 characters long. Valid characters are:<br>a..z<br>A..Z<br>0..9<br>-<br>_<br>Names are case sensitive and must be unique within an AMF network. The name cannot be the word "local" or an abbreviation of the word "local" (such as "l", "lo" etc.). |
| <1-4094>    | An ID number that uniquely identifies this area.                                                                                                                                                                                                                                                     |
| local       | Set the area to be the local area. The local area contains the device you are configuring.                                                                                                                                                                                                           |

**Mode** Global Configuration

**Usage notes** This command enables you to divide your AMF network into areas. Each area is managed by at least one AMF master node. Each area can have up to 120 nodes, depending on the license installed on that area's master node.

The whole AMF network is managed by up to 8 AMF controllers. Each AMF controller can communicate with multiple areas. The number of areas supported on a controller depends on the license installed on that controller.

You must give each area in an AMF network a unique name and ID number.

Only one local area can be configured on a device. You must specify a local area on each controller, remote AMF master, and gateway node.

**Example** To create the AMF area named New-Zealand, with an ID of 1, and specify that it is the local area, use the command:

```
controller-1(config)# atmf area New-Zealand id 1 local
```

To configure a remote area named Auckland, with an ID of 100, use the command:

```
controller-1(config)# atmf area Auckland id 100
```



**Related commands**

- atmf area password
- show atmf area
- show atmf area summary
- show atmf area nodes
- switchport atmf-arealink

**Command changes** Version 5.5.1-2.1: area **id** maximum increased to 4094

# atmf area password

**Overview** This command sets a password on an AMF area.

Use the **no** variant of this command to remove the password.

This command is only valid on AMF controllers, master nodes and gateway nodes. The area name must have been configured first.

**Syntax** `atmf area <area-name> password [8] <password>`  
`no atmf area <area-name> password`

| Parameter   | Description                                                                                                                                                                           |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <area-name> | The AMF area name.                                                                                                                                                                    |
| 8           | This parameter is displayed in <b>show running-config</b> output to indicate that it is displaying the password in encrypted form. You should not enter <b>8</b> on the CLI yourself. |
| <password>  | The password is between 8 and 32 characters long. It can include spaces.                                                                                                              |

**Mode** Global Configuration

**Usage notes** You must configure a password on each area that an AMF controller communicates with, except for the controller's local area. The areas must already have been created using the [atmf area](#) command.

Enter the password identically on both of:

- the area that locally contains the controller, and
- the remote AMF area masters

The command **show running-config atmf** will display the encrypted version of this password. The encryption keys will match between the controller and the remote AMF master.

If multiple controller and masters exist in an area, they must all have the same area configuration.

**Example** To give the AMF area named *Auckland* a password of "secure#1" use the following command on the controller:

```
controller-1(config)# atmf area Auckland password secure#1
```

and also use the following command on the master node for the Auckland area:

```
auck-master(config)# atmf area Auckland password secure#1
```

**Related  
commands**

- atmf area
- show atmf area
- show atmf area summary
- show atmf area nodes
- switchport atmf-arealink

# atmf authorize

**Overview** On an AMF network, with secure mode enabled, use this command on an AMF master to authorize an AMF node to join the network. AMF nodes waiting to be authorized appear in the pending authorization queue, which can be examined using the [show atmf authorization](#) command with the **pending** parameter.

Use the **no** variant of this command to revoke authorization for an AMF node on an AMF master.

**Syntax** `atmf authorize {<node-name> [area <area-name>]|all-pending}`  
`no atmf authorize <node-name> [area <area-name>]`

| Parameter   | Description                                                              |
|-------------|--------------------------------------------------------------------------|
| <node-name> | The name of the node to be authorized or have its authorization revoked. |
| area        | Specify an AMF area.                                                     |
| <area-name> | This is the name of the area the node belongs to.                        |
| all-pending | Authorize all nodes in the pending queue.                                |

**Mode** Privileged Exec

**Usage notes** On an AMF controller, AMF remote-area masters must be authorized by the controller, and the AMF remote-area masters will also need to authorized access from the AMF controller.

**Example** To authorize all AMF nodes in the pending authorization queue on an AMF master, use the command:

```
awplus# atmf authorize all-pending
```

To authorize a node called "node2" in remote AMF area "area3", use the command:

```
awplus# atmf authorize node2 area "area3"
```

To authorize a node called "node4" on an AMF master, use the command:

```
awplus# atmf authorize node4
```

To revoke authorization for a node called "node4" on an AMF master, use the command:

```
awplus# no atmf authorize node4
```

**Related commands** [atmf secure-mode](#)  
[clear atmf secure-mode certificates](#)  
[show atmf authorization](#)  
[show atmf secure-mode](#)

show atmf secure-mode certificates

show atmf secure-mode statistics

**Command**    Version 5.4.7-0.3: command added  
**changes**

# atmf authorize provision

**Overview** Use this command from an AMF controller or AMF master to pre-authorize a node on an AMF network running in secure mode. This allows a node to join the AMF network the moment the [atmf secure-mode](#) command is run on that node.

Use the **no** variant of this command to remove a provisional authorization from and AMF controller or AMF master.

**Syntax**

```
atmf authorize provision [timeout <minutes>] node <node-name>
interface <interface-name> [area <area-name>]

atmf authorize provision [timeout <minutes>] mac <mac-address>

atmf authorize provision [timeout <minutes>] all

no atmf authorize provision node <node-name> interface
<interface-name> [area <area-name>]

no atmf authorize provision mac <mac-address>

no atmf authorize provision all
```

| Parameter        | Description                                                                                                            |
|------------------|------------------------------------------------------------------------------------------------------------------------|
| timeout          | Timeout for provisional authorization. Authorization for provisioned nodes expires after the timeout period specified. |
| <minutes>        | Timeout in minutes. A value between 1 and 6000 is permissible with the default being 60 minutes.                       |
| node             | Specify a node to provision by node name.                                                                              |
| <node-name>      | The name of the node to provisionally authorize.                                                                       |
| interface        | Specify the interface the node will connect on.                                                                        |
| <interface-name> | The name of the interface, this can be a switchport, link aggregator, LACP link, or virtual link.                      |
| area             | Specify the AMF area.                                                                                                  |
| <area-name>      | This is the name of the area the node belongs to.                                                                      |
| mac              | Specify a node to provision by MAC address.                                                                            |
| <mac-address>    | Enter a MAC address to provisionally authorize in the format HHHH.HHHH.HHHH.                                           |
| all              | Provision authorization for all secure mode capable nodes.                                                             |

**Default** The default timeout is 60 minutes.

**Mode** Privileged Exec

**Example** To provisionally authorize all non-secure AMF nodes, use the command:

```
awplus# atmf authorize provision all
```

To authorize a node with a MAC address of 0000.cd28.0880 for 2 hours, use the command:

```
awplus# authorize provision timeout 120 mac 0000.cd28.0880
```

To remove all provisional authorization, on an AMF master, use the command:

```
awplus# no atmf authorize provision all
```

**Related commands**

- [show atmf authorization](#)
- [show atmf secure-mode](#)

**Command changes**

- Version 5.4.7-0.3: command added

# atmf backup

**Overview** This command can only be applied to a master node. It manually schedules an AMF backup to start at a specified time and to execute a specified number of times per day.

Use the **no** variant of this command to disable the schedule.

**Syntax** `atmf backup {default|<hh:mm> frequency <1-24>}`

| Parameter        | Description                                                                                                            |
|------------------|------------------------------------------------------------------------------------------------------------------------|
| default          | Restore the default backup schedule.                                                                                   |
| <hh:mm>          | Sets the time of day to apply the first backup, in hours and minutes. Note that this parameter uses the 24 hour clock. |
| backup           | Enables AMF backup to external media.                                                                                  |
| frequency <1-24> | Sets the number of times within a 24 hour period that backups will be taken.                                           |

**Default** Backups run daily at 03:00 AM, by default

**Mode** Global Configuration

**Usage notes** Running this command only configures the schedule. To enable the schedule, you should then apply the command [atmf backup enable](#).

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

**Example** To schedule backup requests to begin at 11 am and execute twice per day (11 am and 11 pm), use the following command:

```
node_1# configure terminal
node_1(config)# atmf backup 11:00 frequency 2
```

**CAUTION:** File names that comprise identical text, but with differing case, such as *Test.txt* and *test.txt*, will not be recognized as being different on FAT32 based backup media such as a USB storage device. However, these filenames will be recognized as being different on your Linux based device. Therefore, for good practice, ensure that you apply a consistent case structure for your back-up file names.

**Related commands** [atmf backup enable](#)  
[atmf backup stop](#)  
[show atmf backup](#)



# atmf backup area-masters delete

**Overview** Use this command to delete from external media, a backup of a specified node in a specified area.

Note that this command can only be run on an AMF controller.

**Syntax** `atmf backup area-masters delete area <area-name> node <node-name>`

| Parameter                      | Description                                                   |
|--------------------------------|---------------------------------------------------------------|
| <code>&lt;area-name&gt;</code> | The area that contains the node whose backup will be deleted. |
| <code>&lt;node-name&gt;</code> | The node whose backup will be deleted.                        |

**Mode** Privileged Exec

**Example** To delete the backup of the remote area-master named “well-gate” in the AMF area named Wellington, use the command:

```
controller-1# atmf backup area-masters delete area Wellington
node well-gate
```

**Related commands** [show atmf backup area](#)

# atmf backup area-masters enable

**Overview** Use this command to enable backup of remote area-masters from the AMF controller. This command is only valid on AMF controllers.

Use the **no** form of the command to stop backups of remote area-masters.

**Syntax** `atmf backup area-masters enable`  
`no atmf backup area-masters enable`

**Mode** Global configuration

**Default** Remote area backups are disabled by default

**Usage notes** Use the following commands to configure the remote area-master backups:

- [atmf backup](#) to configure when the backups begin and how often they run
- [atmf backup server](#) to configure the backup server.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

**Example** To enable scheduled backups of AMF remote area-masters, use the commands:

```
controller-1# configure terminal
controller-1(config)# atmf backup area-masters enable
```

To disable scheduled backups of AMF remote area-masters, use the commands:

```
controller-1# configure terminal
controller-1(config)# no atmf backup area-masters enable
```

**Related commands** [atmf backup server](#)  
[atmf backup](#)  
[show atmf backup area](#)

# atmf backup area-masters now

**Overview** Use this command to run an AMF backup of one or more remote area-masters from the AMF controller immediately.

This command is only valid on AMF controllers.

**Syntax** `atmf backup area-masters now [area <area-name>|area <area-name>  
node <node-name>]`

| Parameter   | Description                                    |
|-------------|------------------------------------------------|
| <area-name> | The area whose area-masters will be backed up. |
| <node-name> | The node that will be backed up.               |

**Mode** Privileged Exec

**Example** To back up all local master nodes in all areas controlled by controller-1, use the command

```
controller-1# atmf backup area-masters now
```

To back up all local masters in the AMF area named Wellington, use the command

```
controller-1# atmf backup area-masters now area Wellington
```

To back up the local master “well-master” in the Wellington area, use the command

```
controller-1# atmf backup area-masters now area Wellington node
well-master
```

**Related commands** [atmf backup area-masters enable](#)  
[atmf backup area-masters synchronize](#)  
[show atmf backup area](#)

# atmf backup area-masters synchronize

**Overview** Use this command to synchronize backed-up area-master files between the active remote file server and the backup remote file server. Files are copied from the active server to the remote server.

Note that this command is only valid on AMF controllers.

**Syntax** `atmf backup area-masters synchronize`

**Mode** Privileged Exec

**Example** To synchronize backed-up files between the remote file servers for all area-masters, use the command:

```
controller-1# atmf backup area-masters synchronize
```

**Related commands** [atmf backup area-masters enable](#)  
[atmf backup area-masters now](#)  
[show atmf backup area](#)

# atmf backup bandwidth

**Overview** This command sets the maximum bandwidth in kilobytes per second (kBps) available to the AMF backup process. This command enables you to restrict the bandwidth that is utilized for downloading file contents during a backup.

**NOTE:** *This command will only run on an AMF master. An error message will be generated if the command is attempted on node that is not a master.*

*Also note that setting the bandwidth value to zero will allow the transmission of as much bandwidth as is available, which can exceed the maximum configurable speed of 1000 kBps. In effect, zero means unlimited.*

Use the **no** variant of this command to reset (to its default value of zero) the maximum bandwidth in kilobytes per second (kBps) available when initiating an AMF backup. A value of zero tells the backup process to transfer files using unlimited bandwidth.

**Syntax** `atmf backup bandwidth <0-1000>`  
`no atmf backup bandwidth`

| Parameter                   | Description                                       |
|-----------------------------|---------------------------------------------------|
| <code>&lt;0-1000&gt;</code> | Sets the bandwidth in kilobytes per second (kBps) |

**Default** The default value is zero, allowing unlimited bandwidth when executing an AMF backup.

**Mode** Global Configuration

**Examples** To set an atmf backup bandwidth of 750 kBps, use the commands:

```
node2# configure terminal
node2(config)# atmf backup bandwidth 750
```

To set the AMF backup bandwidth to the default value for unlimited bandwidth, use the commands:

```
node2# configure terminal
node2(config)# no atmf backup bandwidth
```

**Related commands** [show atmf backup](#)

# atmf backup delete

**Overview** This command removes the backup file from the external media of a specified AMF node.

Note that this command can only be run from an AMF master node.

**Syntax** `atmf backup delete <node-name>`

| Parameter                      | Description                                         |
|--------------------------------|-----------------------------------------------------|
| <code>&lt;node-name&gt;</code> | The AMF node name of the backup file to be deleted. |

**Mode** Privileged Exec

**Example** To delete the backup file from node2, use the following command:

```
Node_1# atmf backup delete node2
```

**Related commands**

- [show atmf backup](#)
- [atmf backup now](#)
- [atmf backup stop](#)

# atmf backup enable

**Overview** This command enables automatic AMF backups on the AMF master node that you are connected to. By default, automatic backup starts at 3:00 AM. However, this schedule can be changed by the [atmf backup](#) command. Note that backups are initiated and stored only on the master nodes.

Use the **no** variant of this command to disable any AMF backups that have been scheduled and previously enabled.

**Syntax** `atmf backup enable`  
`no atmf backup enable`

**Default** Automatic AMF backup functionality is enabled on the AMF master when it is configured and external media, i.e. an SD card or a USB storage device or remote server, is detected.

**Mode** Global Configuration

**Usage notes** A warning message will appear if you run the [atmf backup enable](#) command with either insufficient or marginal memory availability on your external storage device.

You can use the command [show atmf backup](#) on page 2044 to check the amount of space available on your external storage device.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

**Example** To turn on automatic AMF backup, use the following command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup enable
```

**Related commands** [show atmf](#)  
[show atmf backup](#)  
[atmf backup](#)  
[atmf backup now](#)  
[atmf enable](#)

# atmf backup guests delete

**Overview** This command removes a guest node's backup files from external media such as a USB drive, SD card, or an external file server.

**Syntax** `atmf backup guests delete <node-name> <guest-port>`

| Parameter                       | Description                          |
|---------------------------------|--------------------------------------|
| <code>&lt;node-name&gt;</code>  | The name of the guest's parent node. |
| <code>&lt;guest-port&gt;</code> | The port number on the parent node.  |

**Mode** User Exec/Privileged Exec

**Example** On a parent node named "node1" (which, in this case, the user has a direct console connection to) use the following command to remove the backup files of the guest node that is directly connected to port1.0.3.

```
node1# atmf backup guests delete node1 port1.0.3
```

**Related Command** [atmf backup delete](#)  
[atmf backup area-masters delete](#)  
[show atmf backup guest](#)



# atmf backup guests enable

**Overview** Use this command to enable backups of remote guest nodes from an AMF master.  
Use the **no** variant of this command to disable the ability of the guest nodes to be backed up.

**Syntax** `atmf backup guests enable`  
`no atmf backup guests enable`

**Default** Guest node backups are enabled by default.

**Mode** Global Config

**Usage notes** We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

**Example** On the AMF master node, enable all scheduled guest node backups:

```
atmf-master# configure terminal
atmf-master(config)# atmf backup guests enable
```

**Related commands** [atmf backup area-masters enable](#)  
[show atmf backup guest](#)  
[atmf backup guests synchronize](#)

# atmf backup guests now

**Overview** This command manually triggers an AMF backup of guest nodes on a AMF Master.

**Syntax** `atmf backup guests now [<node-name>] [<guest-port>]`

| Parameter                       | Description                                      |
|---------------------------------|--------------------------------------------------|
| <code>&lt;node-name&gt;</code>  | The name of the guest's parent node.             |
| <code>&lt;guest-port&gt;</code> | The port number that connects to the guest node. |

**Default** n/a

**Mode** Privileged Exec

**Example** Use the following command to manually trigger the backup of all guests in the AMF network

```
awplus# atmf backup guests now
```

**Example** To manually trigger the backup of a guest node connected to port 1.0.23 of node1, use the following command:

```
awplus# atmf backup guests now node1 port1.0.23
```

**Related commands** [show atmf backup guest](#)

# atmf backup guests synchronize

**Overview** This command initiates a manual synchronization of all guest backup file-sets across remote file servers and various redundancy backup media, such as USB storage devices. This facility ensures that each device contains the same backup image files. Note that this backup synchronization process will occur as part of the regular backups scheduled by the [atmf backup](#) command.

**Syntax** `atmf backup guests synchronize`

**Default** n/a

**Mode** User Exec/Privileged Exec

**Example** To synchronize backups across remote file servers and storage devices, use the command:

```
Node1#atmf backup guests synchronize
```

**Related commands** [atmf backup redundancy enable](#)  
[show atmf guests](#)  
[atmf backup guests enable](#)

# atmf backup now

**Overview** This command initiates an immediate AMF backup of either all AMF members, or a selected AMF member. Note that this backup information is stored in the external media on the master node of the device on which this command is run, even though the selected AMF member may not be a master node.

Note that this command can only be run on an AMF master node.

**Syntax** `atmf backup now [<nodename>]`

| Parameter                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;nodename&gt;</code><br>or<br><code>&lt;hostname&gt;</code> | The name of the AMF member to be backed up, as set by the command <code>hostname</code> on page 255. Where no name has been assigned to this device, then you must use the default name, which is the word "host", then an underscore, then (without a space) the MAC address of the device to be backed up. For example <code>host_0016_76b1_7a5e</code> . Note that the node-name appears as the command Prompt when in Privileged Exec mode. |

**Default** A backup is initiated for all nodes on the AMF (but stored on the master nodes).

**Mode** Privileged Exec

**Usage notes** Although this command will select the AMF node to be backed-up, it can only be run from any AMF master node.

**NOTE:** The backup produced will be for the selected node but the backed-up config will reside on the external media of the AMF master node on which the command was run. However, this process will result in the information on one master being more up-to-date. To maintain concurrent backups on both masters, you can apply the `backup now` command to the master working-set. This is shown in Example 4 below.

**Example 1** In this example, an AMF member has not been assigned a host name. The following command is run on the `AMF_Master_2` node to immediately backup the device that is identified by its MAC address of `0016.76b1.7a5e`:

```
AMF_Master_2# atmf backup now host_0016_76b1_7a5e
```

**NOTE:** When a host name is derived from its MAC address, the syntax format entered changes from `XXXX.XXXX.XXXX` to `XXXX_XXXX_XXXX`.

**Example 2** In this example, an AMF member has the host name, **office\_annex**. The following command will immediately backup this device:

```
AMF_Master_2# atmf backup now office_annex
```

This command is initiated on the device's master node named **AMF\_Master\_2** and initiates an immediate backup on the device named **office\_annex**.

**Example 3** To initiate from AMF\_master\_1 an immediate backup of all AMF member nodes, use the following command:

```
AMF_Master_1# amf backup now
```

**Example 4** To initiate an immediate backup of the node with the host-name "office\_annex" and store the configuration on both masters, use the following process:

From the AMF\_master\_1, set the working-set to comprise only of the automatic group, master nodes.

```
AMF_Master_1# atmf working-set group master
```

This command returns the following display:

```
=====
AMF_Master_1, AMF_Master_2
=====

Working set join
```

Backup the AMF member with the host name, **office\_annex** on both the master nodes as defined by the working set.

```
AMF_Master[2]# atmf backup now office_annex
```

Note that the [2] shown in the command prompt indicates a 2 node working-set.

**Related commands**

- [atmf backup](#)
- [atmf backup stop](#)
- [hostname](#)
- [show atmf backup](#)

# atmf backup redundancy enable

**Overview** This command is used to enable or disable AMF backup redundancy.

**Syntax** `atmf backup redundancy enable`  
`no atmf backup redundancy enable`

**Default** Disabled

**Mode** Global Configuration

**Usage notes** If the AMF Master or Controller supports any removable media (SD card/USB), it uses the removable media as the redundant backup for the AMF data backup.

This feature is valid only if remote file servers are configured on the AMF Master or Controller.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

**Example** To enable AMF backup redundancy, use the commands:

```
awplus# configure terminal
awplus(config)# atmf backup redundancy enable
```

To disable AMF backup redundancy, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf backup redundancy enable
```

**Related commands** [atmf backup synchronize](#)  
[show atmf backup](#)  
[show atmf backup area](#)

# atmf backup server

**Overview** This command configures remote file servers as the destination for AMF backups.

Use the **no** variant of this command to remove the destination server(s). When all servers are removed the system will revert to backup from external media.

**Syntax** `atmf backup server id {1|2} <hostlocation> username <username>  
[path <path>|port <1-65535>]  
no atmf backup server id {1|2}`

| Parameter      | Description                                                                                                                                                                                      |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id             | Remote server backup server identifier.                                                                                                                                                          |
| {1 2}          | The backup server identifier number (1 or 2). Note that there can be up to two backup servers, numbered 1 and 2 respectively, and you would need to run this command separately for each server. |
| <hostlocation> | Either the name or the IP address (IPv4 or IPv6) of the selected backup server (1 or 2).                                                                                                         |
| username       | Configure the username to log in with on the selected remote file server.                                                                                                                        |
| <username>     | The selected remote file server's username.                                                                                                                                                      |
| path           | The location of the backup files on the selected remote file server. By default this will be the home directory of the username used to log in with.                                             |
| <path>         | The directory path utilized to store the backup files on the selected remote file server. No spaces are allowed in the path.                                                                     |
| port           | The connection to the selected remote backup file server using SSH. By default SSH connects to a device on TCP port 22 but this can be changed with this command.                                |
| <1-65535>      | A TCP port within the specified range.                                                                                                                                                           |

**Defaults** Remote backup servers are not configured. The default SSH TCP port is 22. The path utilized on the remote file server is the home directory of the username.

**Mode** Global Exec

**Usage notes** The hostname and username parameters must both be configured.

**Examples** To configure server 1 with an IPv4 address and a username of *backup1*, use the commands:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 192.168.1.1
username backup1
```

To configure server 1 with an IPv6 address and a username of *backup1*, use the command:

```
AMF_backup1_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 FFEE::01 username
backup1
```

To configure server 2 with a hostname and username, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com
username backup2
```

To configure server 2 with a hostname and username in addition to the optional path and port parameters, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com
username backup2 path tokyo port 1024
```

To unconfigure the AMF remote backup file server 1, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# no atmf backup server id 1
```

**Related  
commands**   [show atmf backup](#)



# atmf backup stop

**Overview** Running this command stops a backup that is currently running on the master node you are logged onto. Note that if you have two masters and want to stop both, then you can either run this command separately on each master node, or add both masters to a working set, and issue this command to the working set.

Note that this command can only be run on a master node.

**Syntax** `atmf backup stop`

**Mode** Privileged Exec

**Usage notes** This command is used to halt an AMF backup that is in progress. In this situation the backup process will finish on its current node and then stop.

**Example** To stop a backup that is currently executing on master node node-1, use the following command:

```
AMF_Master_1# amf backup stop
```

**Related commands**

- [atmf backup](#)
- [atmf backup enable](#)
- [atmf backup now](#)
- [show atmf backup](#)

# atmf backup synchronize

**Overview** For the master node you are connected to, this command initiates a system backup of files from the node's active remote file server to its backup remote file server. Note that this process happens automatically each time the network is backed up.

Note that this command can only be run from a master node.

**Syntax** `atmf backup synchronize`

**Mode** Privileged Exec

**Example** When connected to the master node AMF\_Master\_1, the following command will initiate a backup of all system related files from its active remote file server to its backup remote file server.

```
AMF_Master_1# atmf backup synchronize
```

**Related commands**

- [atmf backup enable](#)
- [atmf backup redundancy enable](#)
- [show atmf](#)
- [show atmf backup](#)

# atmf cleanup

**Overview** This command is an alias to the [erase factory-default](#) command.

# atmf container

**Overview** Use this command to create or update an AMF container on a Virtual AMF Appliance (VAA) virtual machine.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove an AMF container.

**Syntax** `atmf container <container-name>`  
`no atmf container <container-name>`

| Parameter                           | Description                                                 |
|-------------------------------------|-------------------------------------------------------------|
| <code>&lt;container-name&gt;</code> | The name of the AMF container to create, update, or remove. |

**Mode** AMF Container Configuration

**Usage notes** You cannot delete a container while it is still running. First use the **state disable** command to stop the container.

**Examples** To create or update the AMF container "vac-wlg-1", use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)#
```

To remove the AMF container "vac-wlg-1", use the commands:

```
awplus# configure terminal
awplus(config)# no atmf container vac-wlg-1
```

**Related commands** [area-link](#)  
[atmf container login](#)  
[bridge-group \(amf-container\)](#)  
[description \(amf-container\)](#)  
[show atmf container](#)  
[state](#)

**Command changes** Version 5.4.7-0.1: command added

# atmf container login

**Overview** Use this command to login to an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

**Syntax** `atmf container login <container-name>`

| Parameter                           | Description                                           |
|-------------------------------------|-------------------------------------------------------|
| <code>&lt;container-name&gt;</code> | The name of the AMF container you wish to login into. |

**Mode** Privileged Exec

**Usage notes** If you try to login to a AMF container that has not been created, or is not running, you will see the following message:

```
% Container does not exist or is not running.
```

To exit from a container and return to the host VAA press `<Ctrl+a q>`.

**Example** To login to container “vac-wlg-1”, use the command:

```
awplus# atmf container login vac-wlg-1
```

You will then be presented with a login screen for that container:

```
Connected to tty 1
Type <Ctrl+a q> to exit the console, <Ctrl+a Ctrl+a> to enter Ctrl+a itself

vac-wlg-1 login: manager
Password: friend

AlliedWare Plus (TM) 5.4.7 02/03/17 08:46:12

vac-wlg-1>
```

**Related commands** [atmf container](#)  
[show atmf container](#)

**Command changes** Version 5.4.7-0.1: command added

# atmf controller

**Overview** Use this command to configure the device as an AMF controller. This enables you to split a large AMF network into multiple areas.

AMF controller is a licensed feature. The number of areas supported on a controller depends on the license installed on that controller.

Use the **no** variant of this command to remove the AMF controller functionality.

**Syntax** `atmf controller`  
`no atmf controller`

**Mode** Global configuration

**Usage notes** If a valid AMF controller license is not available on the device, the device will accept this command but will not act as a controller until you install a valid license. The following message will warn you of this:

"An AMF Controller license must be installed before this feature will become active"

**NOTE:** *If the AMF controller functionality is removed from a device using the **no atmf controller** command then the device must be rebooted if it is to function properly as an AMF master.*

**Example** To configure the node named *controller-1* as an AMF controller, use the commands:

```
controller-1# configure terminal
controller-1(config)# atmf controller
```

To stop the node named *controller-1* from being an AMF controller, use the commands:

```
controller-1# configure terminal
controller-1(config)# no atmf controller
```

**Related commands** [atmf area](#)  
[show atmf](#)

# atmf distribute firmware

**Overview** This command can be used to upgrade software one AMF node at a time. A URL can be selected from any media location. The latest compatible release for a node will be selected from this location.

Several procedures are performed to ensure the upgrade will succeed. This includes checking the current node release boots from flash. If there is enough space on flash, the software release is copied to flash on the new location.

The new release name is updated using the **boot system** command. The old release will become the backup release file. If a release file exists in a remote device (such as TFTP or HTTP, for example) then the URL should specify the exact release filename without using a wild card character.

The command will continue to upgrade software until all nodes are upgraded. At the end of the upgrade cycle the command should be used on the working-set.

**Syntax** `atmf distribute firmware <filename>`

| Parameter                     | Description                                                                                                                           |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;filename&gt;</code> | The filename and path of the file. See the <a href="#">File Management Feature Overview and Configuration Guide</a> for valid syntax. |

**Mode** Privileged Exec

**Examples** To upgrade nodes in a AMF network with a predefined AMF group called 'teams', use the following command:

```
Team1# atmf working-set group teams
```

```
=====
Team1, Team2, Team3:
=====
Working set join
```

```
ATMF_NETWORK[3]# atmf distribute firmware card:*.rel
```

```
Retrieving data from Team1
Retrieving data from Team2
Retrieving data from Team3

ATMF Firmware Upgrade:

Node Name New Release File Status

Team1 x510-5.4.7-1.1.rel Release ready
Team2 x930-5.4.7-1.1.rel Release ready
Team3 x930-5.4.7-1.1.rel Release ready
Continue the rolling reboot ? (y/n):y
=====
Copying Release : x510-5.4.7-1.1.rel to Team1
Updating Release : x510-5.4.7-1.1.rel information on Team1
=====
Copying Release : x930-5.4.7-1.1.rel to Team2
Updating Release : x930-5.4.7-1.1.rel information on Team2
=====
Copying Release : x930-5.4.7-1.1.rel to Team3
Updating Release : x930-5.4.7-1.1.rel information on Team3
=====
New firmware will not take effect until nodes are rebooted.
=====

ATMF_NETWORK[3]#
```

**Related commands**   [atmf working-set](#)



# atmf domain vlan

**Overview** The AMF domain VLAN is created when the AMF network is first initiated and is assigned a default VID of 4091. This command enables you to change the VID from this default value on this device.

The AMF domain VLAN is one of AMF's internal VLANs (the management VLAN is the other internal VLAN). AMF uses these internal VLANs to communicate network status information between nodes. These VLANs must be reserved for AMF and not used for other purposes.

An important point conceptually is that although the domain VLAN exists globally across the AMF network, it is assigned separately to each domain. The AMF network therefore can be thought of as comprising a series of domain VLANs each having the same VID and each being applied to a horizontal slice (domain) of the AMF. It follows therefore that the domain VLANs are only applied to ports that form cross-links and not to ports that form uplinks/downlinks.

**CAUTION:** Every member of your AMF network must have the same domain VLAN, management VLAN, and management subnet.

**CAUTION:** If you change the domain VLAN, management VLAN, or management subnet of a node, that change takes effect immediately and the node will immediately leave the AMF network and try to rejoin it. The AMF network will not be complete until you have given all devices the same setting, so they can all rejoin the AMF network.

Use the **no** variant of this command to reset the VLAN ID to its default value of 4091.

**Syntax** `atmf domain vlan <2-4090>`  
`no atmf domain vlan`

| Parameter                   | Description                             |
|-----------------------------|-----------------------------------------|
| <code>&lt;2-4090&gt;</code> | The VLAN number in the range 2 to 4090. |

**Default** VLAN 4091

**Mode** Global Configuration

**Usage notes** We recommend you only change the domain VLAN when first creating the AMF network, and only if VLAN 4091 is already being used in your network.

However, if you do need to change the VLAN on an existing AMF network, use the following steps:

- 1) Create a working set of the whole of your AMF network, using the commands:

```
master# atmf working-set group all
```

You must use **working-set group all** if changing the domain VLAN. If you use a different working-set, nodes that are not in that working-set will lose contact with the AMF network.

- 2) The prompt will display the number of nodes in the AMF network. Record this number. In this example, the network is named "test" and has 10 nodes:

```
test[10]#
```

- 3) Enter the new VLAN ID, using the commands:

```
test[10]# configure terminal
```

```
test(config)[10]# atmf domain vlan <2-4090>
```

The nodes will execute the command in parallel, leave the AMF network, and attempt to rejoin through the new VLAN.

- 4) Create the working set again, using the commands:

```
master(config)# exit
```

```
master# atmf working-set group all
```

- 5) Save the configuration, using the command:

```
test[10]# write
```

- 6) The prompt will display the number of nodes in the AMF network. Check that this is the same as the number in step 1. If it is not, you will need to change the VLAN on missing devices by logging into their consoles directly.

**NOTE:** The domain VLAN will automatically be assigned an IP subnet address based on the value configured by the command *atmf management subnet*.

The default VLAN ID lies outside the user-configurable range. If you need to reset the VLAN to the default VLAN ID, use the **no** variant of this command to do so.

**Examples** To change the AMF domain VLAN to 4090 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
```

```
test[10]# configure terminal
```

```
test(config)[10]# atmf domain vlan 4090
```

```
master(config)# exit
```

```
master# atmf working-set group all
```

```
test[10]# write
```

To reset the AMF domain VLAN to its default of 4091 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# no atmf domain vlan
master(config)# exit
master# atmf working-set group all
test[10]# write
```

**Related commands**

- [atmf management subnet](#)
- [atmf management vlan](#)

# atmf enable

**Overview** This command manually enables (turns on) the AMF feature for the device being configured.

Use the **no** variant of this command to disable (turn off) the AMF feature on the member node.

**Syntax** `atmf enable`  
`no atmf enable`

**Default** Once AMF is configured, the AMF feature starts automatically when the device starts up.

**Mode** Global Configuration

**Usage notes** The device does not auto negotiate AMF domain specific settings such as the Network Name. You should therefore, configure your device with any domain specific (non default) settings before enabling AMF.

**Examples** To turn off AMF, use the command:

```
MyNode# config terminal
MyNode(config)# no atmf enable
```

To turn on AMF, use the command:

```
MyNode(config)# atmf enable
```

This command returns the following display:

```
% Warning: The ATMF network config has been set to enable
% Save the config and restart the system for this change to take
effect.
```

# atmf group (membership)

**Overview** This command configures a device to be a member of one or more AMF groups. Groups exist in three forms: Implicit Groups, Automatic Groups, and User-defined Groups.

- Implicit Groups
  - all: All nodes in the AMF
  - current: The current working-set
  - local: The originating node.

Note that the Implicit Groups do not appear in show group output.

- Automatic Groups - These are defined by hardware architecture, e.g. x510, x230, x8100, AR3050S, AR4050S.
- User-defined Groups - These enable you to define arbitrary groups of AMF members based on your own criteria.

Each node in the AMF is automatically assigned membership to the implicit groups, and the automatic groups that are appropriate to its node type, e.g. x230, PoE. Similarly, nodes that are configured as masters are automatically assigned to the master group.

Use the **no** variant of this command to remove the membership.

**Syntax** `atmf group <group-list>`  
`no atmf group <group-list>`

| Parameter                       | Description                                                                                                                                                  |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;group-list&gt;</code> | A list of group names. These should be entered as a comma delimited list without spaces. Names can contain alphanumeric characters, hyphens and underscores. |

**Mode** Global Configuration

**Usage notes** You can use this command to define your own arbitrary groups of AMF members based on your own network's configuration requirements. Applying a node to a non existing group will result in the group automatically being created.

Note that the master nodes are automatically assigned to be members of the pre-existing master group.

The following example configures the device to be members of three groups; two are company departments, and one comprises all devices located in building\_2. To avoid having to run this command separately on each device that is to be added to these groups, you can remotely assign all of these devices to a working-set, then use the capabilities of the working-set to apply the [atmf group \(membership\)](#) command to all members of the working set.

**Example 1** To specify the device to become a member of AMF groups named *marketing*, *sales*, and *building\_2*, use the following commands:

```
node-1# configure terminal
node-1(config)# atmf group marketing,sales,building_2
```

**Example 2** To add the nodes *member\_node\_1* and *member\_node\_2* to groups *building1* and *sales*, first add the nodes to the working-set:

```
master_node# atmf working-set member_node_1,member_node_2
```

This command returns the following output confirming that the nodes *member\_node\_1* and *member\_node\_2* are now part of the working-set:

```
=====
member_node_1, member_node_2
=====

Working set join
```

Then add the members of the working set to the groups:

```
atmf-net[2]# configure terminal
atmf-net[2](config)# atmf group building1,sales
atmf-net[2](config)# exit
atmf-net[2]# show atmf group
```

This command returns the following output displaying the groups that are members of the working-set.

```
=====
member_node_1
=====

AMF group information

building1, sales
```

**Related commands** [show atmf group](#)  
[show atmf group members](#)

# atmf guest-class

**Overview** This modal command creates a guest-class. Guest-classes are modal templates that can be applied to selected guest types. Once you have created a guest-class, you can select it by entering its mode. From here, you can then configure a further set of operational settings specifically for the new guest-class.

These settings can then all be applied to a guest link by running the [switchport atmf-guestlink](#) command. The following settings can be configured from each guest class mode:

- discovery method
- model type
- http-enable setting
- guest port, user name, and password

The **no** variant of this command removes the guest-class. Note that you cannot remove a guest-class that is assigned to a port.

**Syntax** `atmf guest-class <guest-class-name>`  
`no atmf guest-class <guest-class-name>`

| Parameter                             | Description                                                                                                    |
|---------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <code>&lt;guest-class-name&gt;</code> | The name assigned to the guest-class type. This can be chosen from an arbitrary string of up to 15 characters. |

**Mode** Global Configuration

**Example** To create a guest-class named 'camera' use the commands:

```
node1# configure terminal
node1(config)# atmf guest-class camera
node1(config-atmf-guest)#
```

To remove the guest-class named 'camera' use the commands:

```
node1# configure terminal
node1(config)# no atmf guest-class camera
```

**Related commands** [show atmf area guests](#)  
[discovery](#)  
[firmware-url](#)  
[http-enable](#)  
[username \(atmf-guest\)](#)  
[modeltype](#)

```
switchport atmf-guestlink
show atmf links guest
show atmf guests
login-fallback enable
```



# atmf log-verbose

**Overview** This command limits the number of log messages displayed on the console or permanently logged.

Use the **no** variant of this command to reset to the default.

**Syntax** `atmf log-verbose <1-3>`  
`no atmf log-verbose`

| Parameter | Description                                         |
|-----------|-----------------------------------------------------|
| <1-3>     | The verbose limitation (3 = noisiest, 1 = quietest) |

**Default** The default log display is 3.

**Usage** This command is intended for use in large networks where verbose output can make the console unusable for periods of time while nodes are joining and leaving.

**Mode** Global Configuration

**Example** To set the log-verbose to noise level 2, use the command:

```
node-1# configure terminal
node-1(config)# atmf log-verbose 2
```

**Validation Command** `show atmf`

# atmf management subnet

**Overview** This command is used to assign a subnet that will be allocated to the AMF management and domain management VLANs. From the address space defined by this command, two subnets are created, a management subnet component and a domain component, as explained in the Usage section below.

AMF uses these internal IPv4 subnets to communicate network status information between nodes. These subnet addresses must be reserved for AMF and not used for other purposes.

**CAUTION:** Every member of your AMF network must have the same domain VLAN, management VLAN, and management subnet.

**CAUTION:** If you change the domain VLAN, management VLAN, or management subnet of a node, that change takes effect immediately and the node will immediately leave the AMF network and try to rejoin it. The AMF network will not be complete until you have given all devices the same setting, so they can all rejoin the AMF network.

Use the **no** variant of this command to remove the assigned subnet.

**Syntax** `atmf management subnet <a.b.0.0>`  
`no atmf management subnet`

| Parameter                    | Description                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;a.b.0.0&gt;</code> | The IP address selected for the management subnet. Because a mask of 255.255.0.0 (i.e. /16) will be applied automatically, an IP address in the format a.b.0.0 must be selected. Usually this subnet address is selected from an appropriate range from within the private address space of 172.16.0.0 to 172.31.255.255, or 192.168.0.0, as defined in RFC1918. |

**Default** 172.31.0.0. A subnet mask of 255.255.0.0 will automatically be applied.

**Mode** Global Configuration

**Usage notes** Running this command will result in the creation of a further two subnets (within the class B address space assigned) and the mask will extend from /16 to /17.

For example, if the management subnet is assigned the address 172.31.0.0/16, this will result in the automatic creation of the following two subnets:

- 172.31.0.0/17 assigned to the [atmf management vlan](#)
- 172.31.128.0/17 assigned to the [atmf domain vlan](#).

We recommend you only change the management subnet when first creating the AMF network, and only if 172.31.0.0 is already being used in your network.

However, if you do need to change the subnet on an existing AMF network, use the following steps:

- 1) Create a working set of the whole of your AMF network, using the commands:

```
master# atmf working-set group all
```

You must use **working-set group all** if changing the domain VLAN, management VLAN, or management subnet. If you use a different working-set, nodes that are not in that working-set will lose contact with the AMF network.

- 2) The prompt will display the number of nodes in the AMF network. Record this number. In this example, the network is named "test" and has 10 nodes:

```
test[10]#
```

- 3) Enter the new subnet address, using the commands:

```
test[10]# configure terminal
```

```
test(config)[10]# atmf management subnet <a.b.0.0>
```

The nodes will execute the command in parallel, leave the AMF network, and attempt to rejoin through the new subnet.

- 4) Create the working set again, using the commands:

```
master(config)# exit
```

```
master# atmf working-set group all
```

- 5) Save the configuration, using the command:

```
test[10]# write
```

- 6) The prompt will display the number of nodes in the AMF network. Check that this is the same as the number in step 1. If it is not, you will need to change the subnet on missing devices by logging into their consoles directly.

**Examples** To change the AMF management subnet address to 172.25.0.0 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
```

```
test[10]# configure terminal
```

```
test(config)[10]# atmf management subnet 172.25.0.0
```

```
master(config)# exit
```

```
master# atmf working-set group all
```

```
test[10]# write
```

To reset the AMF management subnet address to its default of 172.31.0.0 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# no atmf management subnet
master(config)# exit
master# atmf working-set group all
test[10]# write
```

**Related commands**   [atmf domain vlan](#)  
[atmf management vlan](#)

# atmf management vlan

**Overview** The AMF management VLAN is created when the AMF network is first initiated and is assigned a default VID of 4092. This command enables you to change the VID from this default value on this device.

The AMF management VLAN is one of AMF's internal VLANs (the domain VLAN is the other internal VLAN). AMF uses these internal VLANs to communicate network status information between nodes. These VLANs must be reserved for AMF and not used for other purposes.

**CAUTION:** Every member of your AMF network must have the same domain VLAN, management VLAN, and management subnet.

**CAUTION:** If you change the domain VLAN, management VLAN, or management subnet of a node, that change takes effect immediately and the node will immediately leave the AMF network and try to rejoin it. The AMF network will not be complete until you have given all devices the same setting, so they can all rejoin the AMF network.

Use the **no** variant of this command to restore the VID to the default of 4092.

**Syntax** `atmf management vlan <2-4090>`  
`no atmf management vlan`

| Parameter                   | Description                                  |
|-----------------------------|----------------------------------------------|
| <code>&lt;2-4090&gt;</code> | The VID assigned to the AMF management VLAN. |

**Default** VLAN 4092

**Mode** Global Configuration

**Usage notes** We recommend you only change the management VLAN when first creating the AMF network, and only if VLAN 4092 is already being used in your network.

However, if you do need to change the VLAN on an existing AMF network, use the following steps to ensure you change it on all nodes simultaneously:

- 1) Create a working set of the whole of your AMF network, using the commands:

```
master# atmf working-set group all
```

You must use **working-set group all** if changing the management VLAN. If you use a different working-set, nodes that are not in that working-set will lose contact with the AMF network.

- 2) The prompt will display the number of nodes in the AMF network. Record this number. In this example, the network is named "test" and has 10 nodes:

```
test[10]#
```

- 3) Enter the new VLAN ID, using the commands:

```
test[10]# configure terminal
test(config)[10]# atmf management vlan <2-4090>
```

The nodes will execute the command in parallel, leave the AMF network, and attempt to rejoin through the new VLAN.

- 4) Create the working set again, using the commands:

```
master(config)# exit
master# atmf working-set group all
```

- 5) Save the configuration, using the command:

```
test[10]# write
```

- 6) The prompt will display the number of nodes in the AMF network. Check that this is the same as the number in step 1. If it is not, you will need to change the VLAN on missing devices by logging into their consoles directly.

**NOTE:** The management VLAN will automatically be assigned an IP subnet address based on the value configured by the command [atmf management subnet](#).

The default VLAN ID lies outside the user-configurable range. If you need to reset the VLAN to the default VLAN ID, use the **no** variant of this command to do so.

**Examples** To change the AMF management VLAN to 4090 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# atmf management vlan 4090
master(config)# exit
master# atmf working-set group all
test[10]# write
```

To reset the AMF management VLAN to its default of 4092 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# no atmf management vlan
master(config)# exit
master# atmf working-set group all
test[10]# write
```

**Related commands** [atmf domain vlan](#)  
[atmf management subnet](#)

# atmf master

**Overview** This command configures the device to be an AMF master node and automatically creates an AMF master group. The master node is considered to be the core of the AMF network, and must be present for the AMF to form. The AMF master has its node depth set to 0. Note that the node depth vertical distance is determined by the number of uplinks/downlinks that exist between the node and its master.

An AMF master node must be present for an AMF network to form. Up to two AMF master nodes may exist in a network, and they **must** be connected by an AMF crosslink.

**NOTE:** Master nodes are an essential component of an AMF network. In order to run AMF, an AMF License is required for each master node.

If the crosslink between two AMF masters fails, then one of the masters will become isolated from the rest of the AMF network.

Use the **no** variant of this command to remove the device as an AMF master node. The node will retain its node depth of 0 until the network is rebooted.

**NOTE:** Node depth is the vertical distance (or level) from the master node (whose depth value is 0).

**Syntax** `atmf master`  
`no atmf master`

**Default** The device is not configured to be an AMF master node.

**Mode** Global Configuration

**Example** To specify that this node is an AMF master, use the following command:

```
node-1# configure terminal
node-1(config)# atmf master
```

**Related commands** [show atmf](#)  
[show atmf group](#)

## atmf mtu

**Overview** This command configures the AMF network Maximum Transmission Unit (MTU). The MTU value will be applied to the AMF Management VLAN, the AMF Domain VLAN and AMF Area links.

Use the **no** variant of this command to restore the default MTU.

**Syntax** `atmf mtu <1300-1442>`  
`no atmf mtu`

| Parameter                      | Description                                                                                                                               |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;1300-1442&gt;</code> | The value of the maximum transmission unit for the AMF network, which sets the maximum size of all AMF packets generated from the device. |

**Default** 1300

**Mode** Global Configuration

**Usage notes** The default value of 1300 will work for all AMF networks (including those that involve virtual links over IPsec tunnels). If there are virtual links over IPsec tunnels anywhere in the AMF network, we recommend not changing this default. If there are no virtual links over IPsec tunnels, then this AMF MTU value may be increased for network efficiency.

**Example** To change the ATMF network MTU to 1442, use the command:

```
awplus(config)# atmf mtu 1442
```

**Related commands** [show atmf detail](#)



# atmf network-name

**Overview** This command applies an AMF network name to a (prospective) AMF node. In order for an AMF network to be valid, its network-name must be configured on at least two nodes, one of which must be configured as a master and have an AMF License applied. These nodes may be connected using either AMF downlinks or crosslinks.

For more information on configuring an AMF master node, see the command [atmf master](#).

Use the **no** variant of this command to remove the AMF network name.

**Syntax** `atmf network-name <name>`  
`no atmf network-name`

| Parameter                 | Description                                                                              |
|---------------------------|------------------------------------------------------------------------------------------|
| <code>&lt;name&gt;</code> | The AMF network name. Up to 15 printable characters can be entered for the network-name. |

**Mode** Global Configuration

**Usage notes** This is one of the essential commands when configuring AMF and must be entered on each node that is to be part of the AMF.

A switching node (master or member) may be a member of only one AMF network.

**CAUTION:** *Ensure that you enter the correct network name. Entering an incorrect name will cause the AMF network to fragment (at the next reboot).*

**Example** To set the AMF network name to `amf_net` use the command:

```
Node_1(config)# atmf network-name amf_net
```

# atmf provision (interface)

**Overview** This command configures a specified port on an AMF node to accept a provisioned node, via an AMF link, some time in the future.

Use the **no** variant of this command to remove the provisioning on the node.

**Syntax** `atmf provision <nodename>`  
`no atmf provision`

| Parameter                     | Description                                                                         |
|-------------------------------|-------------------------------------------------------------------------------------|
| <code>&lt;nodename&gt;</code> | The name of the provisioned node that will appear on the AMF network in the future. |

**Mode** Interface Configuration for a switchport, a static aggregator, dynamic channel group or an Eth port on an AR-Series device.

**Usage notes** The port should be configured as an AMF link or cross link and should be 'down' to add or remove a provisioned node.

**Example** To provision an AMF node named node1 for port1.0.1, use the commands:

```
host1(config)# interface port1.0.1
host1(config-if)# atmf provision node1
```

**Related commands**

- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [configure boot config \(amf-provision\)](#)
- [configure boot system \(amf-provision\)](#)
- [copy \(amf-provision\)](#)
- [create \(amf-provision\)](#)
- [delete \(amf-provision\)](#)
- [identity \(amf-provision\)](#)
- [license-cert \(amf-provision\)](#)
- [locate \(amf-provision\)](#)
- [show atmf provision nodes](#)
- [show atmf links](#)
- [switchport atmf-link](#)
- [switchport atmf-crosslink](#)

# atmf provision node

**Overview** Use this command to provision a replacement node for a specified interface. Node provisioning is effectively the process of creating a backup file-set on a master node that can be loaded onto a provisioned node some time in the future. This file-set is created just as if the provisioned node really existed and was connected to the network. Typically these comprise configuration, operating system, and license files etc.

You can optionally provision a node with multiple device-type backups. When a device is then attached to the network, AMF uses its device-type to find the correct configuration to use. For example you can create an x510 and an x530 provisioning configuration for a node called 'node1' and if either an x510 or an x530 is attached to that node the appropriate configuration will be used.

Use the **no** variant of this command to remove a provisioned node.

**Syntax** `atmf provision node <nodename> [device <device-type>]`  
`no atmf provision node <nodename> [device <device-type>]`

| Parameter     | Description                                                                                                                                                   |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <nodename>    | The name of the provisioned node that will appear on the AMF network.                                                                                         |
| device        | Optionally specify a device type.                                                                                                                             |
| <device-type> | Any valid device type e.g. AR3050s, ie200, x950. For a full list of valid device types use the command <b>atmf provision node &lt;nodename&gt; device ?</b> . |

**Mode** Privileged Exec

**Usage notes** This command creates the directory structure for the provisioned node's file-set. It also switches to the AMF provision node prompt so that the nodes backup file-set can be created or updated. This is typically done with the [create \(amf-provision\)](#) or [clone \(amf-provision\)](#) commands.

For more information on AMF provisioning, see the [AMF Feature Overview and Configuration Guide](#)..

**Example** To configure node named 'node1', use the command:

```
awplus# atmf provision node node1
awplus(atmf-provision) #
```

To configure a node named 'node1' for device type 'x530', use the command:

```
awplus# atmf provision node node1 device x530
awplus(atmf-provision) #
```

**Related commands**

- atmf provision (interface)
- clone (amf-provision)
- configure boot config (amf-provision)
- configure boot system (amf-provision)
- copy (amf-provision)
- create (amf-provision)
- delete (amf-provision)
- identity (amf-provision)
- license-cert (amf-provision)
- locate (amf-provision)
- show atmf provision nodes

**Command changes**    Version 5.4.9-0.1: command added

# atmf reboot-rolling

**Overview** This command enables you to reboot the nodes in an AMF working-set, one at a time, as a rolling sequence in order to minimize downtime. Once a rebooted node has finished running its configuration and its ports are up, it re-joins the AMF network and the next node is rebooted.

By adding the `url` parameter, you can also upgrade your devices' software one AMF node at a time.

The **force** parameter forces the rolling reboot to continue even if a previous node does not rejoin the AMF network. Without the **force** parameter, the unsuitable node will time-out and the rolling reboot process will stop. However, with the **force** parameter applied, the process will ignore the timeout and move on to reboot the next node in the sequence.

This command can take a significant amount of time to complete.

**Syntax** `atmf reboot-rolling [force] [<url>]`

| Parameter                | Description                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>force</code>       | Ignore a failed node and move on to the next node. Where a node fails to reboot a timeout is applied based on the time taken during the last reboot. |
| <code>&lt;url&gt;</code> | The path to the software upgrade file.                                                                                                               |

**Mode** Privileged Exec

**Usage notes** You can load the software from a variety of locations. The latest compatible release for a node will be selected from your selected location, based on the parameters and URL you have entered.

For example `usb:/5.5.2-2/x*-5.5.2-2-*.rel` will select from the folder `usb:/5.5.2-2` the latest file that matches the selection `x(wildcard)-5.5.2-2-(wildcard).rel`. Because `x*` is applied, each device type will be detected and its appropriate release file will be installed.

Other allowable entries are:

| Entry                                 | Used when loading software                              |
|---------------------------------------|---------------------------------------------------------|
| <code>card:*.rel:</code>              | from an SD card                                         |
| <code>tftp:&lt;ip-address&gt;:</code> | from a TFTP server                                      |
| <code>usb:</code>                     | from a USB flash drive                                  |
| <code>flash:</code>                   | from flash memory, e.g. from one x930 switch to another |
| <code>scp:</code>                     | using secure copy                                       |
| <code>http:</code>                    | from an HTTP file server                                |

Several checks are performed to ensure the upgrade will succeed. These include checking the current node release boots from flash. If there is enough space on flash, the software release is copied to flash to a new location on each node as it is processed. The new release name will be updated using the **boot system<release-name>** command, and the old release will become the backup release file.

**NOTE:** *If you are using TFTP or HTTP, for example, to access a file on a remote device then the URL should specify the exact release filename without using wild card characters.*

On bootup the software release is verified. Should an upgrade fail, the upgrading unit will revert back to its previous software version. At the completion of this command, a report is run showing the release upgrade status of each node.

**NOTE:** *Take care when removing external media or rebooting your devices. Removing an external media while files are being written entails a significant risk of causing a file corruption.*

**Example 1** To reboot all x530 nodes in an AMF network, use the commands:

```
Bld2_Floor_1# atmf working-set group x530
```

This command returns the following type of screen output:

```
=====
node1, node2, node3:
=====

Working set join

AMF_NETWORK[3]#
```

```
ATMF_NETWORK[3]# atmf reboot-rolling
```

When the reboot has completed, a number of status screens appear. The selection of these screens will depend on the parameters set.

```
Bld2_Floor_1#atmf working-set group x530
```

```
=====
SW_Team1, SW_Team2, SW_Team3:
=====
```

```
Working set join
```

```
ATMF_NETWORK[3]#atmf reboot-rolling
ATMF Rolling Reboot Nodes:
```

| Node Name | Timeout<br>(Minutes) |
|-----------|----------------------|
|-----------|----------------------|

|          |    |
|----------|----|
| SW_Team1 | 14 |
| SW_Team2 | 8  |
| SW_Team3 | 8  |

```
Continue the rolling reboot ? (y/n):y
```

```
=====
ATMF Rolling Reboot: Rebooting SW_Team1
=====
```

```
% SW_Team1 has left the working-set
Reboot of SW_Team1 has completed
=====
```

```
ATMF Rolling Reboot: Rebooting SW_Team2
=====
```

```
% SW_Team2 has left the working-set
Reboot of SW_Team2 has completed
=====
```

```
ATMF Rolling Reboot: Rebooting SW_Team3
=====
```

```
% SW_Team3 has left the working-set
Reboot of SW_Team3 has completed
=====
```

```
ATMF Rolling Reboot Complete
```

| Node Name | Reboot Status |
|-----------|---------------|
|-----------|---------------|

|          |          |
|----------|----------|
| SW_Team1 | Rebooted |
| SW_Team2 | Rebooted |
| SW_Team3 | Rebooted |

**Example 2** To update firmware on all relevant devices in the network, when the new files are for 5.5.2-2.1 and are stored in a directory on a USB stick, use the commands:

```
Node_1# atmf working-set group all
```

```
ATMF_NETWORK[9]# atmf reboot-rolling
usb:/5.5.2-2/x*-5.5.2-2*.rel
```

| ATMF Rolling Reboot Nodes:           |                      |                    |               |
|--------------------------------------|----------------------|--------------------|---------------|
| Node Name                            | Timeout<br>(Minutes) | New Release File   | Status        |
| -----                                |                      |                    |               |
| SW_Team1                             | 8                    | x530-5.5.2-2.1.rel | Release Ready |
| SW_Team2                             | 10                   | x530-5.5.2-2.1.rel | Release Ready |
| SW_Team3                             | 8                    | ---                | Not Supported |
| HW_Team1                             | 6                    | ---                | Incompatible  |
| Bld1_Floor_2                         | 2                    | x930-5.5.2-2.1.rel | Release Ready |
| Bld1_Floor_1                         | 4                    | ---                | Incompatible  |
| Building_1                           | 2                    | ---                | Incompatible  |
| Building_2                           | 2                    | x950-5.5.2-2.1.rel | Release Ready |
| Continue upgrading releases ? (y/n): |                      |                    |               |



# atmf recover

**Overview** This command is used to manually initiate the recovery (or replication) of an AMF node, usually when a node is being replaced.

**Syntax** `atmf recover [<node-name> master <node-name>]`  
`atmf recover [<node-name> controller <node-name>]`

| Parameter                           | Description                                                                                                                                                                                                                              |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;node-name&gt;</i>            | The name of the device whose configuration is to be recovered or replicated.                                                                                                                                                             |
| master<br><i>&lt;node-name&gt;</i>  | The name of the master device that holds the required configuration information.<br>Note that although you can omit both the node name and the master name; you cannot specify a master name unless you also specify the node name.      |
| controller <i>&lt;node-name&gt;</i> | The name of the controller that holds the required configuration information.<br>Note that although you can omit both the node name and the controller name; you cannot specify a controller name unless you also specify the node name. |

**Mode** Privileged Exec

**Usage notes** The recovery/replication process involves loading the configuration file for a node that is either about to be replaced or has experienced some problem. You can specify the configuration file of the device being replaced by using the *<node-name>* parameter, and you can specify the name of the master node or controller holding the configuration file.

If the *<node-name>* parameter is not entered then the node will attempt to use one that has been previously configured. If the replacement node has no previous configuration (and has no previously used node-name), then the recovery will fail.

If the master or controller name is not specified then the device will poll all known AMF masters and controllers and execute an election process (based on the last successful backup and its timestamp) to determine which to use. If no valid backup master or controller is found, then this command will fail.

No error checking occurs when this command is run. Regardless of the last backup status, the recovering node will attempt to load its configuration from the specified master node or controller.

If the node has previously been configured, we recommend that you suspend any AMF backup before running this command. This is to prevent corruption of the backup files on the AMF master as it attempts to both backup and recover the node at the same time.

**Example** To recover the AMF node named Node\_10 from the AMF master node named Master\_2, use the following command:

```
Master_2# atmf recover Node_10 master Master_2
```

**Related commands**

- atmf backup stop
- show atmf backup
- show atmf

# atmf recover guest

**Overview** Use this command to initiate a guest node recovery or replacement by reloading its backup file-set that is located within the AMF backup system. Note that this command must be run on the edge node device that connects to the guest node.

**Syntax** `atmf recover guest [<guest-port>]`

| Parameter                       | Description                                      |
|---------------------------------|--------------------------------------------------|
| <code>&lt;guest-port&gt;</code> | The port number that connects to the guest node. |

**Mode** User Exec/Privileged Exec

**Example** To recover a guest on node1 port1.0.1, use the following command

```
node1# atmf recover guest port1.0.1
```

**Related commands** [show atmf backup guest](#)

# atmf recover led-off

**Overview** This command turns off the recovery failure flashing port LEDs. It reverts the LED's function to their normal operational mode, and in doing so assists with resolving the recovery problem. You can repeat this process until the recovery failure has been resolved. For more information, see the [AMF Feature Overview and Configuration Guide](#).

**Syntax** `atmf recover led-off`

**Default** Normal operational mode

**Mode** Privileged Exec

**Example** To revert the LEDs on Node1 from recovery mode display to their normal operational mode, use the command:

```
Node1# atmf recover led-off
```

**Related commands** [atmf recover](#)

# atmf recover over-eth

**Overview** Use this command to enable AMF recovery over an AR-series device's Eth port. This setting persists even after restoring a device to a 'clean' state with the [erase factory-default](#) or [atmf cleanup](#) command.

Use the **no** variant of this command to disable AMF recover over an Eth port.

**Syntax** `atmf recover over-eth`  
`no atmf recover over-eth`

**Default** Eth ports cannot be used for recovery.

**Mode** Privileged Exec

**Usage notes** AMF links over Eth ports are only available if your network is running in AMF secure mode (see [atmf secure-mode](#) for more information on AMF secure mode).

**Example** To enable AMF recovery over an Eth port, use the command:

```
awplus# atmf recover over-eth
```

To disable AMF recovery over an Eth port, use the commands:

```
awplus# no atmf recover over-eth
```

**Related commands** [atmf-link](#)  
[atmf recover](#)  
[atmf secure-mode](#)  
[erase factory-default](#)  
[show atmf detail](#)

**Command changes** Version 5.5.0-1.1: command added

# atmf recovery-server

**Overview** Use this command on an AMF master to process recovery requests from isolated AMF nodes. An isolated node is an AMF member that is only connected to the rest of the AMF network via a virtual-link.

This option allows these nodes, which have no AMF neighbors, to be identified for recovery or provisioning purposes. They are identified using an identity token which is stored on the AMF master.

Use the **no** variant of this command to disable processing of recovery requests from isolated AMF nodes.

**Syntax** `atmf recovery-server`  
`no atmf recovery-server`

**Default** Recovery-server is disabled by default.

**Mode** Global Configuration

**Usage notes** Once **recovery-server** is enabled on an AMF network, the next time an isolated node is backed up its identity token will be stored in the AMF master's database. Should the device fail it can then be replaced and auto-recovery will occur as long as:

- the AMF master is accessible to the isolated node, and
- either, a DHCP server is configured to send the Uniform Resource Identifier (URI) of the AMF master to the recovering node, or
- a DNS server is configured to resolve the default recovery URI (`https://amfrecovery.alliedtelesis.com`) to the IP address of the AMF master.

Provisioning of isolated nodes is achieved by creating an identity token for the new node using the [identity \(amf-provision\)](#) command.

See the [AMF Feature Overview and Configuration Guide](#) for information on preparing your network for recovering or provisioning isolated nodes.

**Example** To enable recovery-server on an AMF master, use the commands:

```
awplus# configure terminal
awplus(config)# atmf recovery-server
```

To disable recovery-server on an AMF master, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf recovery-server
```

**Related commands** [atmf backup](#)  
[atmf cleanup](#)  
[identity \(amf-provision\)](#)  
[atmf virtual-link](#)

**Command changes** Version 5.4.7-2.1: command added

# atmf remote-login

**Overview** Use this command to remotely login to other AMF nodes in order to run commands as if you were a local user of that node.

**Syntax** `atmf remote-login [user <name>] <nodename>`

| Parameter  | Description                                            |
|------------|--------------------------------------------------------|
| <name>     | The name of a user on the remote node.                 |
| <nodename> | The name of the remote AMF node you are connecting to. |

**Mode** Privileged Exec (This command will only run at privilege level 15)

**Usage notes** You do not need a valid login on the local device in order to run this command. The session will take you to the enable prompt on the new device. If the remote login session exits for any reason (e.g. device reboot) you will be returned to the originating node.

You can create additional user accounts on nodes. AMF's goal is to provide a uniform management plane across the whole network, so we recommend you use the same user accounts on all the nodes in the network.

In reality, though, it is not essential to have the same accounts on all the nodes. Users can remote login from one node to a second node even if they are logged into the first node with a user account that does not exist on the second node (provided that [atmf restricted-login](#) is disabled and the user account on the first node has privilege level 15).

Moreover, it is possible to use a RADIUS or TACACS+ server to manage user authentication, so users can log into AMF nodes using user accounts that are present on the RADIUS or TACACS+ server, and not present in the local user databases of the AMF nodes.

The software will not allow you to run multiple remote login sessions. You must exit an existing session before starting a new one.

If you disconnect from the VTY session without first exiting from the AMF remote session, the device will keep the AMF remote session open until the [exec-timeout](#) time expires (10 minutes by default). If the exec-timeout time is set to infinity (**exec-timeout 0 0**), then the device is unable to ever close the remote session. To avoid this, we recommend you use the **exit** command to close AMF remote sessions, instead of closing the associated VTY sessions. We also recommend you avoid setting the exec-timeout to infinity.

**Example** To remotely login from node Node10 to Node20, use the following command:

```
Node10# atmf remote-login node20
Node20>
```



To close the session on Node20 and return to Node10's command line, use the following command:

```
Node20# exit
```

```
Node10#
```

In this example, user User1 is a valid user of node5. They can remotely login from node5 to node3 by using the following commands:

```
node5# atmf remote-login user User1 node3
```

```
node3> enable
```

**Related commands** [atmf restricted-login](#)

**Command changes** Version 5.4.6-2.1: changes to AMF user account requirements

# atmf restricted-login

**Overview** By default, users who are logged into any node on an AMF network are able to manage any other node by using either working-sets or an AMF remote login. If the access provided by this feature is too wide, or contravenes network security restrictions, it can be limited by running this command, which changes the access so that:

- users who are logged into non-master nodes cannot execute any commands that involve working-sets, and
- from non-master nodes, users can use remote-login, but only to login to a user account that is valid on the remote device (via a statically configured account or RADIUS/TACACS+). Users are also required to enter the password for that user account.

Once entered on any AMF master node, this command will propagate across the network.

Use the **no** variant of this command to disable restricted login on the AMF network. This allows access to the **atmf working-set** command from any node in the AMF network.

**Syntax** `atmf restricted-login`  
`no atmf restricted-login`

**Mode** Privileged Exec

**Default** Master nodes operate with **atmf restricted-login** disabled.  
Member nodes operate with **atmf restricted-login** enabled.

**NOTE:** The default conditions of this command vary from those applied by its “no” variant. This is because the restricted-login action is only applied by **master** nodes, and in the absence of a master node, the default is to apply the restricted action to all **member** nodes with AMF configured.

**Usage notes** In the presence of a **master** node, its default of **atmf restricted-login disabled** will propagate to all its member nodes. Similarly, any change in this command’s status that is made on a master node, will also propagate to all its member nodes

Note that once you have run this command, certain other commands that utilize the AMF working-set command, such as the **include**, **atmf reboot-rolling** and **show atmf group members** commands, will operate only on master nodes.

Restricted-login must be enabled on AMF areas with more than 120 nodes.

**Example** To enable restricted login, use the command

```
Node_20(config)# atmf restricted-login node20
```

**Related commands** [atmf remote-login](#)  
[show atmf](#)

**Command changes** Version 5.4.6-2.1: changes to AMF user account requirements

# atmf retry guest-link

**Overview** Use this command to retry an AMF guest-link by restarting AMF guest discovery on a port if it is currently in the failed state.

If no port is specified then all configured AMF guest-link ports that are in the failed state are retried.

If a port is specified then that port will only be retried if it is both:

- configured as an AMF guest-link, and
- it is currently in the failed state.

**Syntax** `atmf retry guest-link [<interface>]`

| Parameter                      | Description                                                              |
|--------------------------------|--------------------------------------------------------------------------|
| <code>&lt;interface&gt;</code> | Name of the interface the guest-link you want to retry is configured on. |

**Mode** Privileged Exec

**Example** To retry all configured AMF guest-link currently in a failed state, use the command:

```
awplus# atmf retry guest-link
```

To retry an AMF guest-link configured on port1.0.2 currently in a failed state, use the command:

```
awplus# atmf retry guest-link port1.0.2
```

**Related commands** [show atmf links guest](#)  
[switchport atmf-guestlink](#)

# atmf secure-mode

**Overview** Use this command to enable AMF secure mode on an AMF node. AMF secure mode makes an AMF network more secure by:

- Adding an authorization mechanism before and AMF member is allowed to join an AMF network.
- The encryption of all AMF packets sent between AMF nodes.
- Adding support for user login authentication by RADIUS or TACACS+, and removing the requirement to have the same privileged user account in the local user database on all devices in the AMF network.
- Adding additional logging which enables network administrators to monitor attempts to gain unauthorized access to the AMF network.

Once the secure mode command is run on all nodes on an AMF network, the AMF masters and AMF controllers manage the addition of AMF nodes and AMF areas to the AMF network.

Use the **no** variant of this command to disable AMF secure mode on an AMF node.

**Syntax** `atmf secure-mode`  
`no atmf secure-mode`

**Default** Secure mode is disabled by default.

**Mode** Global Configuration

**Usage notes** When an AMF network is running in AMF secure mode the [atmf restricted-login](#) feature is automatically enabled. This restricts the [atmf working-set](#) command to users that are logged on to an AMF master. This feature cannot be disabled independently of secure mode.

When AMF secure mode is enabled the AMF controllers and masters in the AMF network form a group of certificate authorities. A node may only join a secure AMF network once it has been authorized by a master or controller. When enabled, all devices in the AMF network must be running in secure mode. Unsecured devices will not be able to join a secure AMF network.

**Example** To enable AMF secure mode on an AMF node, use the commands:

```
awplus# configure terminal
awplus(config)# atmf secure-mode
```

To disable AMF secure mode on an AMF node, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf secure-mode
```

**Related commands** [atmf authorize](#)  
[atmf secure-mode certificate expiry](#)

clear atmf secure-mode certificates  
clear atmf secure-mode statistics  
show atmf  
show atmf authorization  
show atmf secure-mode  
show atmf secure-mode certificates  
show atmf secure-mode sa  
show atmf secure-mode statistics

**Command changes**    Version 5.4.7-0.3: command added

# atmf secure-mode certificate expire

**Overview** Use this command on an AMF master to expire a secure mode certificate. Running this command will force the removal of the AMF node from the network.

**Syntax** `atmf secure-mode certificate expire <node-name> [area <area-name>]`

| Parameter                      | Description                                                            |
|--------------------------------|------------------------------------------------------------------------|
| <code>&lt;node-name&gt;</code> | Name of the AMF node you want to expire the certificate for.           |
| <code>area</code>              | Specify an AMF area.                                                   |
| <code>&lt;area-name&gt;</code> | Name of the AMF area you want to expire the AMF nodes certificate for. |

**Mode** Privileged Exec

**Example** To remove an AMF node named “node3” from an AMF network, use the following command on the AMF master:

```
awplus# atmf secure-mode certificate expire node3
```

To remove an AMF node named “node2” in an area named “area2”, use the following command on the AMF master:

```
awplus# atmf secure-mode certificate expire node2 area area2
```

**Related commands**

- [atmf secure-mode](#)
- [show atmf secure-mode](#)
- [show atmf secure-mode certificates](#)

**Command changes** Version 5.4.7-0.3: command added

# atmf secure-mode certificate expiry

**Overview** Use this command to set the expiry time of AMF secure mode certificates. Once an AMF node's certificate expires it must re-authorize and obtain a new certificate from the AMF master.

Use the **no** variant of this command to reset the expiry time to 180 days.

**Syntax** `atmf secure-mode certificate expiry {<days>|infinite}`  
`no atmf secure-mode certificate expiry`

| Parameter                 | Description                                                                                            |
|---------------------------|--------------------------------------------------------------------------------------------------------|
| <code>&lt;days&gt;</code> | Length of time, in days, that an AMF secure mode certificate remains valid. A value between 1 and 365. |
| <code>infinite</code>     | The authorization certificate does not expire, in other words AMF nodes stay authorized indefinitely.  |

**Default** The default expiry time is 180 days.

**Mode** Global Configuration

**Example** To set AMF secure mode certificate expiry to 7 days, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# atmf secure-mode certificate expiry 7
```

To set AMF secure mode certificates to never expire, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# atmf secure-mode certificate expiry infinite
```

To reset the certificate expiry to 180 days, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no atmf secure-mode certificate expiry
```

**Related commands** [atmf secure-mode](#)  
[show atmf secure-mode](#)  
[show atmf secure-mode certificates](#)

**Command changes** Version 5.4.7-0.3: command added



# atmf secure-mode certificate renew

**Overview** Use this command to force all local certificates to expire and be renewed on an AMF secure mode network.

Secure mode certificates renew automatically but this command could be used to renew a certificate in a situation where the automatic renewal may happen while the device is not attached to the AMF network.

**Syntax** `atmf secure-mode certificate renew`

**Mode** Privileged Exec

**Example** To renew a local certificate on a AMF member or AMF master, use the command:

```
awplus# atmf secure-mode certificate renew
```

**Related commands** [show atmf secure-mode certificates](#)  
[show atmf secure-mode statistics](#)

**Command changes** Version 5.4.7-0.3: command added

# atmf secure-mode enable-all

**Overview** Use this command to enable AMF secure mode on an entire network. AMF secure mode makes an AMF network more secure by:

- Adding an authorization mechanism before an AMF member is allowed to join an AMF network.
- The encryption of all AMF packets sent between AMF nodes.
- Adding support for user login authentication by RADIUS or TACACS+, and removing the requirement to have the same privileged user account in the local user database on all devices in the AMF network.
- Adding additional logging which enables network administrators to monitor attempts to gain unauthorized access to the AMF network.

Once this command is run on an AMF network, the AMF masters and AMF controllers manage the addition of AMF nodes and AMF areas to the AMF network.

This command can only be run on an AMF master.

Use the **no** variant of this command to disable AMF secure mode on an entire network.

**Syntax** `atmf secure-mode enable-all`  
`no atmf secure-mode enable-all`

**Default** Secure mode is disabled by default.

**Mode** Privileged Exec

**Usage notes** When an AMF network is running in AMF secure mode the [atmf restricted-login](#) feature is automatically enabled. This restricts the [atmf working-set](#) command to users that are logged on to an AMF master. This feature cannot be disabled independently of secure mode.

When AMF secure mode is enabled the AMF controllers and masters in the AMF network form a group of certificate authorities. A node may only join a secure AMF network once it has been authorized by a master or controller. When enabled, all devices in the AMF network must be running in secure mode. Unsecured devices will not be able to join a secure AMF network.

Running **atmf secure-mode enable-all**:

- Groups all AMF members in a working set.
- Executes [clear atmf secure-mode certificates](#) on the working set of members, which removes existing secure mode certificates from all the nodes.
- Groups all the AMF masters in a working set.
- Executes [atmf authorize provision all](#) on the working set of masters, so all masters provision all nodes.
- Groups all AMF nodes in a working set.

- Runs a script which executes `atmf secure-mode` and then writes the configuration file on each node.
- Starts a timer that ticks every 10 seconds, for a maximum of 10 times, and checks if all the secure mode capable nodes rejoin the AMF network.

Running **no atmf secure-mode enable-all**:

- Groups all AMF nodes in a working set.
- Runs a script which executes **no atmf secure-mode** and then writes the configuration file on each node.
- Starts a timer that ticks every 10 seconds, for a maximum of 10 times, and checks if all the secure mode capable nodes rejoin the AMF network.

**NOTE:** Enabling or disabling secure mode on the network saves the running-config on every device.

**Example** To enable AMF secure mode on the entire network, use the command:

```
awplus# atmf secure-mode enable-all
```

You will be prompted to confirm the action:

```
Total number of nodes 21
21 nodes support secure-mode

Enable secure-mode across the AMF network ? (y/n): y
```

To disable AMF secure mode on the entire network, use the command:

```
awplus# no atmf secure-mode enable-all
```

You will be prompted to confirm the action:

```
% Warning: All security certificates will be deleted.
Disable secure-mode across the AMF network ? (y/n): y
```

**Related commands** `show atmf`

**Command changes** Version 5.4.7-0.3: command added

# atmf select-area

**Overview** Use this command to access devices in an area outside the core area on the controller network. This command will connect you to the remote area-master of the specified area.

This command is only valid on AMF controllers.

The **no** variant of this command disconnects you from the remote area-master.

**Syntax** `atmf select-area {<area-name>|local}`  
`no atmf select-area`

| Parameter                      | Description                                                   |
|--------------------------------|---------------------------------------------------------------|
| <code>&lt;area-name&gt;</code> | Connect to the remote area-master of the area with this name. |
| <code>local</code>             | Return to managing the local controller area.                 |

**Mode** Privileged Exec

**Usage notes** After running this command, use the [atmf working-set](#) command to select the set of nodes you want to access in the remote area.

**Example** To access nodes in the area Canterbury, use the command

```
controller-1# atmf select-area Canterbury
```

This displays the following output:

```
Test_network[3]#atmf select-area Canterbury
=====
Connected to area Canterbury via host Avensis:
=====
```

To return to the local area for controller-1, use the command

```
controller-1# atmf select-area local
```

Alternatively, to return to the local area for controller-1, use the command

```
controller-1# no atmf select-area
```

**Related commands** [atmf working-set](#)

# atmf topology-gui enable

**Overview** Use this command to enable the operation of Vista Manager EX on the Master device.

Vista Manager EX delivers state-of-the-art monitoring and management for your Autonomous Management Framework™ (AMF) network, by automatically creating a complete topology map of switches, firewalls and wireless access points (APs). An expanded view includes third-party devices such as security cameras.

Use the **no** variant of this command to disable operation of Vista Manager EX.

**Syntax** `atmf topology-gui enable`  
`no atmf topology-gui enable`

**Default** Disabled by default on AMF Master and member nodes. Enabled by default on Controllers.

**Mode** Global Configuration mode

**Usage notes** To use Vista Manager EX, you must also enable the HTTP service on all AMF nodes, including all AMF masters and controllers. The HTTP service is enabled by default on AlliedWare Plus switches and disabled by default on AR-Series firewalls. To enable it, use the commands:

```
Node1# configure terminal
Node1(config)# service http
```

On one master in each AMF area in your network, you also need to configure the master to send event notifications to Vista Manager EX. To do this, use the commands:

```
Node1# configure terminal
Node1(config)# log event-host <ip-address> atmf-topology-event
```

**Examples** To enable Vista Manager EX on Node1, use the commands:

```
Node1# configure terminal
Node1(config)# atmf topology-gui enable
```

To disable Vista Manager EX on Node1, use the commands:

```
Node1# configure terminal
Node1(config)# no atmf topology-gui enable
```

**Related commands** [atmf enable](#)  
[log event-host](#)  
[service http](#)

# atmf trustpoint

- Overview** Use this command to set a PKI trustpoint for an AMF network. This command needs to be run on an AMF master or controller.
- The self-signed certificate authority (CA) certificate is distributed to every node on the AMF network. It is used to verify client certificates signed by the trustpoint.
- Use the **no** variant of this command to remove an AMF trustpoint.

**Syntax** `atmf trustpoint <trustpoint-name>`  
`no atmf trustpoint <trustpoint-name>`

| Parameter                            | Description             |
|--------------------------------------|-------------------------|
| <code>&lt;trustpoint-name&gt;</code> | Name of the trustpoint. |

**Default** No trustpoint is configured by default.

**Mode** Global Configuration

**Usage notes** Before using the **atmf trustpoint** command you will need to establish a trustpoint. For example, you can create a local self-signed trustpoint using the procedure outlined below.

Create a self-signed trustpoint called 'our\_trustpoint' with keypair 'our\_key':

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint our_trustpoint
awplus(ca-trustpoint)# enrollment selfsigned
awplus(ca-trustpoint)# rsakeypair our_key
awplus(ca-trustpoint)# exit
awplus(config)# exit
```

Create the root and server certificates for this trustpoint:

```
awplus# crypto pki authenticate our_trustpoint
awplus# crypto pki enroll our_trustpoint
```

For more information about the AlliedWare Plus implementation of Public Key Infrastructure (PKI), see the [Public Key Infrastructure \(PKI\) Feature Overview and Configuration Guide](#)

**Example** To configure an AMF trustpoint for the trustpoint 'our\_trustpoint', use the commands:

```
awplus# configure terminal
awplus(config)# atmf trustpoint our_trustpoint
```

To remove an AMF trustpoint for the trustpoint 'our\_trustpoint', use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no atmf trustpoint our_trustpoint
```

**Related  
commands**

[crypto pki trustpoint](#)

[show atmf](#)

**Command  
changes**

Version 5.4.7-2.1: command added

# atmf virtual-crosslink

**Overview** Use this command to create a virtual crosslink. A virtual crosslink connects an AMF master or controller on a physical device to a Virtual AMF Appliance (VAA) master or controller.

All AMF master nodes must reside in the same AMF domain and are required to be directly connected using AMF crosslinks. In order to be able to meet this requirement for AMF masters running on VAAs, a virtual crosslink connects the AMF master or controller on the physical device to the master or controller on the VAA.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove a virtual crosslink.

**Syntax**

```
atmf virtual-crosslink id <local-id> ip <local-ip> remote-id
<remote-id> remote-ip <remote-ip>

atmf virtual-crosslink id <local-id> ip <local-ip> remote-id
<remote-id> remote-host <domainname>

no atmf virtual-crosslink id <local-id>
```

| Parameter                   | Description                                               |
|-----------------------------|-----------------------------------------------------------|
| id <local-id>               | ID of the local tunnel port, a value between 1 and 4094.  |
| ip <local-ip>               | IPv4 address of the local tunnel port in a.b.c.d format.  |
| remote-id<br><remote-id>    | ID of the remote tunnel port, a value between 1 and 4094. |
| remote-ip<br><remote-ip>    | IPv4 address of the remote tunnel port in a.b.c.d format. |
| remote-host<br><domainname> | The domain name of the remote node.                       |

**Default** No AMF virtual crosslinks are created by default.

**Mode** Global Configuration

**Usage notes** This command allows a virtual tunnel to be created between two remote sites over a Layer 3 link. The tunnel encapsulates AMF packets and allows them to be sent transparently across a Wide Area Network (WAN) such as the Internet.

Configuration involves creating a local tunnel ID, a local IP address, a remote tunnel ID, and a remote IP address or domain name. Each side of the tunnel must be configured with the same, but mirrored parameters.



**NOTE:** *Virtual crosslinks are not supported on AMF container masters, therefore if multiple tenants on a single VAA host are configured for secure mode, only a single AMF master is supported per area.*

**Example** To setup a virtual link from a local site, 'siteA', to a remote site, 'siteB', (assuming there is already IP connectivity between the sites), run the following commands at the local site:

```
siteA# configure terminal
siteA(config)# atmf virtual-crosslink id 5 ip 192.168.100.1
remote-id 10 remote-ip 192.168.200.1
```

At the remote site, run the commands:

```
siteB# configure terminal
siteB(config)# atmf virtual-crosslink id 10 ip 192.168.200.1
remote-id 5 remote-ip 192.168.100.1
```

To remove this virtual crosslink, run the following commands on the local site:

```
siteA# configure terminal
siteA(config)# no atmf virtual-crosslink id 5
```

On the remote site, run the commands:

```
siteB# configure terminal
siteB(config)# no atmf virtual-crosslink id 10
```

**Related commands**

- [atmf virtual-crosslink](#)
- [show atmf links](#)
- [switchport atmf-crosslink](#)

**Command changes**

- Version 5.5.2-0.1: **remote-host** parameter added
- Version 5.4.7-0.3: command added

# atmf virtual-link

**Overview** This command creates one or more Layer 2 tunnels that enable AMF nodes to transparently communicate across a wide area network using Layer 2 connectivity protocols.

Once connected through the tunnel, the remote member will have the same AMF capabilities as a directly connected AMF member.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove the specified virtual link.

**Syntax**

```
atmf virtual-link id <1-4094> ip <a.b.c.d> remote-id <1-4094>
remote-ip <a.b.c.d> [remote-area <area-name>]

atmf virtual-link id <1-4094> interface <interface-name>
remote-id <1-4094> remote-ip <a.b.c.d> [remote-area
<area-name>]

atmf virtual-link id <1-4094> ip <a.b.c.d> remote-id <1-4094>
remote-host <domainname> [remote-area <area-name>]

atmf virtual-link id <1-4094> interface <interface-name>
remote-id <1-4094> remote-host <domainname> [remote-area
<area-name>]

no atmf virtual-link id <1-4094>
```

| Parameter                     | Description                                                                                                                                                                                                                                                       |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id <1-4094>                   | ID of the local tunnel point, in the range 1 to 4094.                                                                                                                                                                                                             |
| ip <a.b.c.d>                  | Specify the local IP address of the local interface for the virtual-link (alternatively you can specify the interface's name, see below).                                                                                                                         |
| interface<br><interface-name> | Specify the local interface name for the virtual-link. This allows you to use a dynamic, rather than a static, local IP address.                                                                                                                                  |
| remote-id<br><1-4094>         | The ID of the (same) tunnel that will be applied by the remote node. Note that this must match the local-id that is defined on the remote node. This means that (for the same tunnel) the local and remote tunnel IDs are reversed on the local and remote nodes. |
| remote-ip<br><a.b.c.d>        | The IP address of the remote node.                                                                                                                                                                                                                                |
| remote-host<br><domainname>   | The domain name of the remote node.                                                                                                                                                                                                                               |
| remote-area<br><area-name>    | The name of the remote area connected to this virtual-link.                                                                                                                                                                                                       |

**Mode** Global Configuration

**Usage notes** The Layer 2 tunnel that this command creates enables a local AMF session to appear to pass transparently across a Wide Area Network (WAN) such as the Internet. The addresses configured as the local and remote tunnel IP addresses must have IP connectivity to each other. If the tunnel is configured to connect a head office and branch office over the Internet, typically this would involve using some type of managed WAN service such as a site-to-site VPN. Tunnels are only supported using IPv4.

Configuration involves creating a local tunnel ID, a local IP address, a remote tunnel ID and a remote IP address or domain name. A reciprocal configuration is also required on the corresponding remote device. The local tunnel ID must be unique to the device on which it is configured.

If an interface acquires its IP address dynamically then the local side of the tunnel can be specified by using the interface's name instead of using its IP address. When using a dynamic local address the remote address of the other side of the virtual-link must be configured with either:

- the IP address of the NAT device the dynamically configured interface is behind, or
- 0.0.0.0, if the virtual-link is configured as a secure virtual-link.

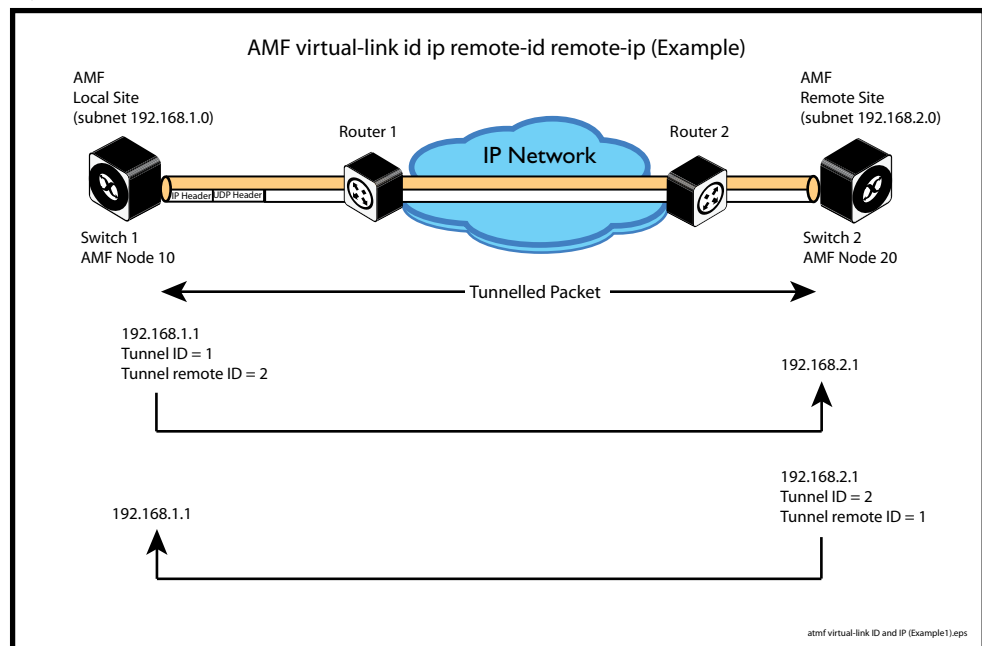
For instructions on how to configure dynamic IP addresses on virtual-links, see the [AMF Feature Overview and Configuration Guide](#).

The tunneled link may operate via external (non AlliedWare Plus) routers in order to provide wide area network connectivity. However in this configuration, the routers perform a conventional router to router connection. The protocol tunneling function is accomplished by the AMF nodes.

**NOTE:** *AMF cannot achieve zero touch replacement of the remote device that terminates the tunnel connection, because you must pre-configure the local IP address and tunnel ID on that remote device.*

**Example 1** Use the following commands to create the tunnel shown in the figure below.

Figure 42-2: AMF virtual link example



```
Node_10(config)# atmf virtual-link id 1 ip 192.168.1.1
remote-id 2 remote-ip 192.168.2.1
```

```
Node_20(config)# atmf virtual-link id 2 ip 192.168.2.1
remote-id 1 remote-ip 192.168.1.1
```

**Example 2** To set up an area virtual link to a remote site (assuming IP connectivity between the sites already), one site must run the following commands:

```
SiteA# configure terminal
SiteA(config)# atmf virtual-link id 5 ip 192.168.100.1
remote-id 10 remote-ip 192.168.200.1 remote-area SiteB-AREA
```

The second site must run the following commands:

```
SiteB# configure terminal
SiteB(config)# atmf virtual-link id 10 ip 192.168.200.1
remote-id 5 remote-ip 192.168.100.1 remote-area SiteA-AREA
```

Before you can apply the above **atmf virtual-link** command, you must configure the area names *SiteB-AREA* and *SiteA-AREA*.

**Related commands**

- [atmf virtual-link description](#)
- [atmf virtual-link protection](#)
- [show atmf](#)
- [show atmf links](#)
- [show atmf virtual-links](#)

**Command changes**

- Version 5.5.2-0.1: **remote-host** parameter added
- Version 5.4.9-0.1: **interface** parameter added

# atmf virtual-link description

**Overview** Use this command to add a description to an existing AMF virtual-link.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove a description from an AMF virtual-link.

**Syntax** `atmf virtual-link id <1-4094> description <description>`  
`no atmf virtual-link id <1-4094> description`

| Parameter                        | Description                         |
|----------------------------------|-------------------------------------|
| <code>id &lt;1-4094&gt;</code>   | ID of the local tunnel point.       |
| <code>&lt;description&gt;</code> | A description for the virtual-link. |

**Default** No description is set by default.

**Mode** Global Configuration

**Example** To add a description to the virtual-link with id '5', use the commands:

```
awplus# configure terminal
awplus(config)# atmf virtual-link id 5 description TO SITE B
```

To remove a description from the virtual-link with id '5', use the commands:

```
awplus# configure terminal
awplus(config)# no atmf virtual-link id 5
```

**Related commands** [atmf virtual-link](#)  
[show atmf links](#)  
[show atmf virtual-links](#)

# atmf virtual-link protection

**Overview** Use this command to add protection to an existing AMF virtual-link. Secure AMF virtual-links encapsulate the L2TPv3 frames of the virtual-link with IPsec.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove protection from an AMF virtual-link.

**Syntax**

```
atmf virtual-link id <1-4094> protection ipsec key [8]
<key-string>

no atmf virtual-link id <1-4094> protection
```

| Parameter    | Description                                                                                                                                                                         |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| id           | Specify the link ID.                                                                                                                                                                |
| <1-4094>     | Link ID in the range 1 to 4094                                                                                                                                                      |
| protection   | Protection is on for this link.                                                                                                                                                     |
| ipsec        | Security provided using IPsec.                                                                                                                                                      |
| key          | Set the shared key.                                                                                                                                                                 |
| 8            | Specifies a string in an encrypted format instead of plain text. The running config will display the new password as an encrypted string even if password encryption is turned off. |
| <key-string> | Specify the shared key for the link.                                                                                                                                                |

**Default** Protection is off by default.

**Mode** Global Configuration

**Usage notes** Considered the following limitations when creating a secure virtual-link:

- Switch devices support a maximum of 20 downstream AMF nodes when using a secure virtual-link as an uplink.
- When there are two or more AMF members behind a shared NAT device, only one of the members will be able to use secure virtual-links.
- An AMF multi-tenant environment supports a maximum cumulative total of 1200 secure virtual-links across all AMF containers.

**Example** To create and configure a virtual link with protection, first create the virtual-link:

```
Host-A# configure terminal

Host-A(config)# atmf virtual-link id 1 ip 192.168.1.1 remote-id
2 remote-ip 192.168.2.1
```

The enable protection on the virtual link:

```
Host-A(config)# atmf virtual-link id 1 protection ipsec key
securepassword
```

Repeat these steps on the other side of the link:

```
Host-B(config)# atmf virtual-link id 2 ip 192.168.2.1 remote-id
1 remote-ip 192.168.1.1
```

```
Host-B(config)# atmf virtual-link id 2 protection ipsec key
securepassword
```

**Related  
commands**

[atmf virtual-link](#)

[show atmf](#)

[show atmf links](#)

[show atmf virtual-links](#)

**Command  
changes**

Version 5.4.9-0.1: command added

# atmf working-set

**Overview** Use this command to execute commands across an individually listed set of AMF nodes or across a named group of nodes.

Note that this command can only be run on a master node.

Use the **no** variant of this command to remove members or groups from the current working-set.

**Syntax** `atmf working-set {[<node-list>]|group  
{<group-list>|all|local|current}}}`  
`no atmf working-set {[<node-list>]|group <group-list>]}`

| Parameter    | Description                                                                                                                                                                                                                      |
|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <node-list>  | A comma delimited list (without spaces) of nodes to be included in the working-set.                                                                                                                                              |
| group        | The AMF group.                                                                                                                                                                                                                   |
| <group-list> | A comma delimited list (without spaces) of groups to be included in the working-set. Note that this can include either defined groups, or any of the Automatic, or Implicit Groups shown earlier in the bulleted list of groups. |
| all          | All nodes in the AMF.                                                                                                                                                                                                            |
| local        | Local node<br>Running this command with the parameters <b>group local</b> will return you to the local prompt and local node connectivity.                                                                                       |
| current      | Nodes in current list.                                                                                                                                                                                                           |

**Mode** Privileged Exec

**Usage notes** You can put AMF nodes into groups by using the [atmf group \(membership\)](#) command.

This command opens a session on multiple network devices. When you change the working set to anything other than the local device, the prompt will change to the AMF network name, followed by the size of the working set, shown in square brackets. This command has to be run at privilege level 15.

In addition to the user defined groups, the following system assigned groups are automatically created:

- Implicit Groups
  - local: The originating node.
  - current: All nodes that comprise the current working-set.
  - all: All nodes in the AMF.



- Automatic Groups - These can be defined by hardware architecture, e.g. x510, x610, x8100, AR3050S or AR4050S, or by certain AMF nodal designations such as master.

Note that the Implicit Groups do not appear in [show atmfgroup](#) command output.

If a node is an AMF master it will be automatically added to the master group.

**Example 1** To add all nodes in the AMF to the working-set, use the command:

```
node1# atmfgroup working-set group all
```

**NOTE:** This command adds the implicit group "all" to the working set, where "all" comprises all nodes in the AMF.

This command displays an output screen similar to the one shown below:

```
=====
node1, node2, node3, node4, node5, node6:
=====

Working set join

ATMF_NETWORK_Name[6]#
```

**Example 2** To return to the local prompt, and connect to only the local node, use the command:

```
ATMF_Network_Name[6]# atmfgroup working-set group local
node1#
```

The following table describes the meaning of the prompts in this example.

| Parameter         | Description                                                                           |
|-------------------|---------------------------------------------------------------------------------------|
| ATMF_Network_Name | The name of the AMF network, as set by the <a href="#">atmf network-name</a> command. |
| [6]               | The number of nodes in the working-set.                                               |
| node1             | The name of the local node, as set by the <a href="#">hostname</a> command.           |

# bridge-group (amf-container)

**Overview** Use this command to connect an AMF container to a bridge created on a Virtual AMF Appliance (VAA) virtual machine for AMF Cloud. This allows the AMF container to connect to a physical network.

Note that this command is only available on AMF Cloud, not on AlliedWare Plus switches.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove a bridge-group from an AMF container.

**Syntax** `bridge-group <bridge-id>`  
`no bridge-group`

| Parameter                      | Description                                                    |
|--------------------------------|----------------------------------------------------------------|
| <code>&lt;bridge-id&gt;</code> | The ID of the bridge group to join, a number between 1 and 64. |

**Mode** AMF Container Configuration

**Usage notes** Each container has two virtual interfaces:

- 1) Interface eth0, used to connect to the AMF controller on the VAA host via an AMF area-link, and configured using this [area-link](#) command.
- 2) Interface eth1, used to connect to the outside world using a bridged L2 network link, and configured using the **bridge-group** command.

Before using this command, a bridge must be created with the same bridge-id on the VAA host using the **bridge <bridge-id>** command.

See the [AMF Feature Overview and Configuration Guide](#) for more information on configuring the bridge.

**Example** To assign a bridge group to AMF container 'vac-wlg-1', use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# bridge-group 1
```

**Related commands** [atmf container](#)  
[show atmf container](#)

**Command changes** Version 5.4.7-0.1: command added

# clear application-proxy threat-protection

**Overview** Use this command to clear the threat protection for a specified address.

**Syntax** `clear application-proxy threat-protection {<ip-address>|<mac-address>|all}`

| Parameter                        | Description                                                                 |
|----------------------------------|-----------------------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code>  | The IPv4 address you wish to clear the threat for, in A.B.C.D format.       |
| <code>&lt;mac-address&gt;</code> | The MAC address you wish to clear the threat for, in HHHH.HHHH.HHHH format. |
| <code>all</code>                 | Clear the threat for all IPv4 and MAC addresses.                            |

**Mode** Privileged Exec

**Example** To clear the threat for 10.34.199.117, use the command:

```
awplus# clear application-proxy threat-protection 10.34.199.117
```

**Related commands**

- [application-proxy quarantine-vlan](#)
- [application-proxy threat-protection](#)
- [application-proxy threat-protection send-summary](#)
- [service atmf-application-proxy](#)
- [show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.2: command added

# clear atmf links

**Overview** Use this command with no parameters to manually reset all the AMF links on a device. You can optionally specify an interface or range of interfaces to reset the links on.

Certain events or topology changes can cause AMF links to be incorrect or outdated. Clearing the links forces AMF to relearn the information from neighboring nodes and create a fresh, correct, view of the network.

**Syntax** `clear atmf links [<interface-list>]`

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface-list> | <p>The interfaces or ports to perform the reset on. An interface-list can be:</p> <ul style="list-style-type: none"><li>• a switchport (e.g. port1.0.1)</li><li>• a static channel group (e.g. sa2)</li><li>• a dynamic (LACP) channel group (e.g. po2)</li><li>• a local port (e.g. of0)</li><li>• You can specify a continuous range of interfaces separated by a hyphen, or a comma-separated list (e.g. port1.0.1, port1.0.4-port1.0.18).</li></ul> <p>The specified interfaces must exist.<br/>If this parameter is left out then all links of the specified type will be reset on the device.</p> |

**Mode** Privileged Exec

**Example** To clear all AMF links on a device, use the following command:

```
awplus# clear atmf links
```

To clear all AMF links on port1.0.1 to port1.0.4 and static aggregator sa1, use the following command:

```
awplus# clear atmf links port1.0.1-port1.0.4,sa1
```

**Related commands** [clear atmf links virtual](#)  
[show atmf links](#)

**Command changes** Version 5.4.8-2.1: command added

# clear atmf links virtual

**Overview** Use this command with no parameters to manually reset all the AMF virtual links on a device. You can, optionally, specify a comma separated list of virtual links to reset.

Certain events or topology changes can cause AMF links to be incorrect or outdated. Clearing the links forces AMF to relearn the information from neighboring nodes and create a fresh, correct view of the network.

**Syntax** `clear atmf links virtual [<virtuallink-list>]`

| Parameter          | Description                                                                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <virtuallink-list> | A single, or list, of AMF virtual link identifiers to reset. This must be a comma separated list of links e.g. <i>vlink1</i> , <i>vlink2</i> , <i>vlink3</i> . Specifying a link range e.g <i>vlink1-vlink3</i> is not supported. |

**Mode** Privileged Exec

**Example** To clear all AMF virtual links on a device, use the following command:

```
awplus# clear atmf links virtual
```

To clear AMF virtual links vlink11 and vlink21, use the following command:

```
awplus# clear atmf links virtual vlink11,vlink22
```

**Related commands** [clear atmf links](#)  
[show atmf links](#)

**Command changes** Version 5.4.8-2.1: command added

# clear atmf links statistics

**Overview** This command resets the values of all AMF link, port, and global statistics to zero.

**Syntax** `clear atmf links statistics`

**Mode** Privilege Exec

**Example** To reset the AMF link statistics values, use the command:

```
node_1# clear atmf links statistics
```

**Related commands** [show atmf links statistics](#)

# clear atmf recovery-file

**Overview** Use this command to delete all of a node's recovery files. It deletes the recovery files stored on:

- the local node,
- neighbor nodes, and
- external media (USB or SD card).

**Syntax** `clear atmf recovery-file`

**Mode** Privileged Exec

**Usage notes** AMF recovery files are created for nodes with special links. Special links include:

- virtual links,
- area links terminating on an AMF master, and
- area virtual links terminating on an AMF master.

An AMF node with one of these special links pushes its startup configuration to its neighbors and to any attached external media. It then fetches and applies this configuration at recovery time. This configuration enables it to contact the AMF master and initiate a recovery.

Recovery files can become out of date if:

- a node's neighbor is off line when changes are made to its configuration, or
- when a node no longer contains a special link.

**Example** To clear a node's recovery files, use the command:

```
node1# clear atmf recovery-file
```

**Output** Figure 42-3: If AlliedWare Plus detects that a node contains a special link then the following message is displayed

```
node1#clear atmf recovery-file
% Warning: ATMF recovery files have been removed.
ATMF recovery may fail. Please save running-configuration.
```

**Related commands** [show atmf recovery-file](#)

**Command changes** Version 5.4.8-0.2: command added



# clear atmf secure-mode certificates

**Overview** Use this command to remove all certificates from an AMF member or master. AMF nodes will need to be re-authorized once this command has been run.

**Syntax** `clear atmf secure-mode certificates`

**Mode** Privileged Exec

**Example** To clear all certificates from an AMF node, use the command:

```
awplus# clear atmf secure-mode certificates
```

If this is the only master on the network you will see the following warning:

```
% Warning: This node is the only master in the network!
All the nodes will become isolated and refuse to join any ATMF
network. The certificates on all the isolated nodes must be
cleared before rejoining an ATMF network will be possible.

To clear certificates a reboot of the device is required.
Clear certificates and Reboot ? (y/n):
```

On an AMF member you will see the following message:

```
To clear certificates a reboot of the device is required.
Clear certificates and Reboot ? (y/n):
```

**Related commands**

- [atmf authorize](#)
- [atmf secure-mode](#)
- [show atmf authorization](#)
- [show atmf secure-mode certificates](#)

**Command changes** Version 5.4.7-0.3: command added

# clear atmf secure-mode statistics

**Overview** Use this command to reset all secure mode statistics to 0.

**Syntax** `clear atmf secure-mode statistics`

**Mode** Privileged Exec

**Example** To reset the AMF secure mode statistics information, use the command:

```
awplus# clear atmf secure-mode statistic
```

**Related commands** [show atmf secure-mode](#)  
[show atmf secure-mode statistics](#)

**Command changes** Version 5.4.7-0.3: command added

# clone (amf-provision)

**Overview** This command sets up a space on the backup media for use with a provisioned node and copies into it almost all files and directories from a chosen backup or provisioned node.

Alternatively, you can set up a new, unique provisioned node by using the command [create \(amf-provision\)](#).

**Syntax** `clone <source-nodename>`

| Parameter                            | Description                                                                        |
|--------------------------------------|------------------------------------------------------------------------------------|
| <code>&lt;source-nodename&gt;</code> | The name of the node whose configuration is to be copied for loading to the clone. |

**Mode** AMF Provisioning

**Usage notes** This command is only available on master nodes in the AMF network.

When using this command it is important to be aware of the following:

- A copy of `<media>:atmf/<atmf_name>/nodes/<source_node>/flash` will be made for the provisioned node and stored in the backup media.
- The directory `<node_backup_dir>/flash/.config/ssh` is excluded from the copy.
- All contents of `<root_backup_dir>/nodes/<nodename>` will be deleted or overwritten.
- Settings for the expected location of other provisioned nodes are excluded from the copy.

The active and backup configuration files are automatically modified in the following ways:

- The **hostname** command is modified to match the name of the provisioned node.
- The **stack virtual-chassis-id** command is removed, if present.

**Example** To copy from the backup of 'device2' to create backup files for the new provisioned node 'device3' use the following command:

```
device1# atmf provision node device3
device1(atmf-provision)# clone device2
```

Figure 42-4: Sample output from the **clone** command

```
device1# atmf provision node device3
device1(atmf-provision)#clone device2
Copying...
Successful operation
```

To confirm that a new provisioned node has been cloned, use the command:

```
device1# show atmf backup
```

The output from this command is shown in the following figure, and shows the details of the new provisioned node 'device3'.

Figure 42-5: Sample output from the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup Enabled
 Schedule 1 per day starting at 03:00
 Next Backup Time 01 Oct 2018 03:00
Backup Bandwidth Unlimited
Backup Media USB (Total 7446.0MB, Free 7297.0MB)
Server Config
 Synchronization Unsynchronized
 Last Run -
 1 Unconfigured
 2 Unconfigured
Current Action Idle
 Started -
 Current Node -

Node Name Date Time In ATMF On Media Status

device3 - - No Yes Prov
device1 30 Sep 2018 00:05:49 No Yes Good
device2 30 Sep 2018 00:05:44 Yes Yes Good
```

**Related  
commands**

[atmf provision \(interface\)](#)  
[atmf provision node](#)  
[configure boot config \(amf-provision\)](#)  
[configure boot system \(amf-provision\)](#)  
[copy \(amf-provision\)](#)  
[create \(amf-provision\)](#)  
[delete \(amf-provision\)](#)  
[identity \(amf-provision\)](#)  
[license-cert \(amf-provision\)](#)  
[locate \(amf-provision\)](#)  
[show atmf provision nodes](#)

**Command  
changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# configure boot config (amf-provision)

**Overview** This command sets the configuration file to use during the next boot cycle. This command can also set a backup configuration file to use if the main configuration file cannot be accessed for an AMF provisioned node. To unset the boot configuration or the backup boot configuration use the **no boot** command.

**Syntax** `configure boot config [backup] <file-path|URL>`  
`configure no boot config [backup]`

| Parameter       | Description                                         |
|-----------------|-----------------------------------------------------|
| backup          | Specify that this is the backup configuration file. |
| <file-path URL> | The path or URL and name of the configuration file. |

**Default** No boot configuration files or backup configuration files are specified for the provisioned node.

**Mode** AMF Provisioning

**Usage notes** When using this command to set a backup configuration file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

**Examples** To set the configuration file 'branch.cfg' on the AMF provisioned node 'node1', use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure boot config
branch.cfg
```

To set the configuration file 'backup.cfg' as the backup to the main configuration file on the AMF provisioned node 'node1', use the command:

```
MasterNodeName(atmf-provision)# configure boot config backup
usb:/atmf/amf_net/nodes/node1/config/backup.cfg
```

To unset the boot configuration, use the command:

```
MasterNodeName(atmf-provision)# configure no boot config
```

To unset the backup boot configuration, use the command:

```
MasterNodeName(atmf-provision)# configure no boot config backup
```

**Related commands**

- [atmf provision \(interface\)](#)
- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [configure boot system \(amf-provision\)](#)
- [create \(amf-provision\)](#)

delete (amf-provision)  
identity (amf-provision)  
license-cert (amf-provision)  
locate (amf-provision)  
show atmf provision nodes

**Command  
changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# configure boot system (amf-provision)

**Overview** This command sets the release file that will load onto a specified provisioned node during the next boot cycle. This command can also set the backup release file to be loaded for an AMF provisioned node. To unset the boot system release file or the backup boot release file use the **no boot** command.

Use the **no** variant of this command to return to the default.

This command can only be run on AMF master nodes.

**Syntax** `configure boot system [backup] <file-path|URL>`  
`configure no boot system [backup]`

| Parameter       | Description                                   |
|-----------------|-----------------------------------------------|
| <file-path URL> | The path or URL and name of the release file. |

**Default** No boot release file or backup release files are specified for the provisioned node.

**Mode** AMF Provisioning

**Usage notes** When using this command to set a backup release file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

**Examples** To set the release file x930-5.4.9-0.1.rel on the AMF provisioned node 'node1', use the command:

```
MasterNodeName# atmf provision node node1
```

```
MasterNodeName(atmf-provision)# configure boot system
x930-5.4.9-0.1.rel
```

To set the backup release file x930-5.4.8-2.5.rel as the backup to the main release file on the AMF provisioned node 'node1', use the command:

```
MasterNodeName# atmf provision node node1
```

```
MasterNodeName(atmf-provision)# configure boot system backup
card:/atmf/amf_net/nodes/node1/flash/x930-5.4.8-2.5.rel
```

To unset the boot release, use the command:

```
MasterNodeName# atmf provision node node1
```

```
MasterNodeName(atmf-provision)# configure no boot system
```

To unset the backup boot release, use the command:

```
MasterNodeName# atmf provision node node1
```

```
MasterNodeName(atmf-provision)# configure no boot system backup
```

**Related commands** [atmf provision \(interface\)](#)

atmf provision node  
clone (amf-provision)  
configure boot config (amf-provision)  
create (amf-provision)  
delete (amf-provision)  
identity (amf-provision)  
license-cert (amf-provision)  
locate (amf-provision)  
show atmf provision nodes

**Command  
changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode



# copy (amf-provision)

**Overview** Use this command to copy configuration and release files for the node you are provisioning.

For more information about using the copy command see [copy \(filename\)](#) in the File and Configuration Management chapter.

**Syntax** `copy [force] <source-name> <destination-name>`

| Parameter                             | Description                                                                                                                                         |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>force</code>                    | This parameter forces the copy command to overwrite the destination file, if it already exists, without prompting the user for confirmation.        |
| <code>&lt;source-name&gt;</code>      | The filename and path of the source file. See the <a href="#">Introduction</a> of the File and Configuration Management chapter for valid syntax.   |
| <code>&lt;destination-name&gt;</code> | The filename and path for the destination file. See <a href="#">Introduction</a> of the File and Configuration Management chapter for valid syntax. |

**Mode** AMF Provisioning

**Example** To copy a configuration file named `current.cfg` from Node\_4's Flash into the `future_node` directory, and set that configuration file to load onto `future_node`, use the following commands:

```
node_4# atmf provision node future_node
node_4(atmf-provision)# create
node_4(atmf-provision)# locate
node_4(atmf-provision)# copy flash:current.cfg
./future_node.cfg
node_4(atmf-provision)# configure boot config future_node.cfg
```

**Related commands**

- [atmf provision \(interface\)](#)
- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [create \(amf-provision\)](#)
- [delete \(amf-provision\)](#)
- [locate \(amf-provision\)](#)
- [show atmf provision nodes](#)

**Command changes** Version 5.4.9-2.1: command added

# create (amf-provision)

**Overview** This command sets up an empty directory on the backup media for use with a provisioned node. This directory can have configuration and release files copied to it from existing devices. Alternatively, the configuration files can be created by the user.

An alternative way to create a new provisioned node is with the command [clone \(amf-provision\)](#).

This command can only run on AMF master nodes.

**Syntax** `create`

**Mode** AMF Provisioning

**Usage notes** This command is only available on master nodes in the AMF network.

A date and time is assigned to the new provisioning directory reflecting when this command was executed. If there is a backup or provisioned node with the same name on another AMF master then the most recent one will be used.

**Example** To create a new provisioned node named "device2" use the command:

```
device1# atmf provision node device2
device1(atmf-provision)# create
```

Running this command will create the following directories:

- `<media>:atmf/<atmf_name>/nodes/<node>`
- `<media>:atmf/<atmf_name>/nodes/<node>/flash`

To confirm the new node's settings, use the command:

```
device1# show atmf backup
```

The output for the **show atmf backup** command is shown in the following figure, and shows details for the new provisioned node 'device2'.

Figure 42-6: Sample output from the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup Enabled
 Schedule 1 per day starting at 03:00
 Next Backup Time 01 Oct 2018 03:00
Backup Bandwidth Unlimited
Backup Media USB (Total 7446.0MB, Free 7315.2MB)
Server Config
 Synchronization Unsynchronized
 Last Run -
 1 Unconfigured
 2 Unconfigured
Current Action Idle
 Started -
 Current Node -

Node Name Date Time In ATMF On Media Status

device2 - - No Yes Prov
device1 30 Sep 2018 00:05:49 No Yes Good
```

For instructions on how to configure on a provisioned node, see the [AMF Feature Overview and Configuration Guide](#).

**Related  
commands**

[atmf provision \(interface\)](#)  
[atmf provision node](#)  
[clone \(amf-provision\)](#)  
[copy \(amf-provision\)](#)  
[configure boot config \(amf-provision\)](#)  
[configure boot system \(amf-provision\)](#)  
[delete \(amf-provision\)](#)  
[identity \(amf-provision\)](#)  
[license-cert \(amf-provision\)](#)  
[locate \(amf-provision\)](#)  
[show atmf provision nodes](#)

**Command  
changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# debug atmf

**Overview** This command enables the AMF debugging facilities, and displays information that is relevant (only) to the current node. The detail of the debugging displayed depends on the parameters specified.

If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

The **no** variant of this command disables either all AMF debugging information, or only the particular information as selected by the command's parameters.

**Syntax**

```
debug atmf
[link|crosslink|arealink|database|neighbor|error|all]

no debug atmf
[link|crosslink|arealink|database|neighbor|error|all]
```

| Parameter | Description                                                                       |
|-----------|-----------------------------------------------------------------------------------|
| link      | Output displays debugging information relating to uplink or downlink information. |
| crosslink | Output displays all crosslink events.                                             |
| arealink  | Output displays all arealink events.                                              |
| database  | Output displays only notable database events.                                     |
| neighbor  | Output displays only notable AMF neighbor events.                                 |
| error     | Output displays AMF error events.                                                 |
| all       | Output displays all AMF events.                                                   |

**Default** All debugging facilities are disabled.

**Mode** User Exec and Global Configuration

**Usage notes** If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

**NOTE:** An alias to the **no** variant of this command is [undebbug atmf](#) on page 2125.

**Examples** To enable all AMF debugging, use the command:

```
node_1# debug atmf
```

To enable AMF uplink and downlink debugging, use the command:

```
node_1# debug atmf link
```

To enable AMF error debugging, use the command:

```
node_1# debug atmf error
```

**Related** no debug all  
**commands**

# debug atmf packet

**Overview** This command configures AMF Packet debugging parameters. The debug only displays information relevant to the current node. The command has following parameters:

**Syntax** debug atmf packet [direction {rx|tx|both}] [level {1|2|3}]  
[timeout <seconds>] [num-pkts <quantity>]  
[filter {node <name>|interface <ifname>}]  
[pkt-type [1][2][3][4][5][6][7][8][9][10][11][12][13]]

## Simplified Syntax

|                   |        |                                                           |
|-------------------|--------|-----------------------------------------------------------|
| debug atmf packet |        | [direction {rx tx both}]                                  |
|                   |        | [level {[1][2 3]}]                                        |
|                   |        | [timeout <seconds>]                                       |
|                   |        | [num-pkts <quantity>]                                     |
| debug atmf packet | filter | [node <name>]                                             |
|                   |        | [interface <ifname>]                                      |
|                   |        | [pkt-type<br>[1][2][3][4][5][6][7][8][9][10][11][12][13]] |

**NOTE:** You can combine the syntax components shown, but when doing so, you must retain their original order.

**Default** Level 1, both Tx and Rx, a timeout of 60 seconds with no filters applied.

**NOTE:** An alias to the **no** variant of this command - [undebug atmf](#) - can be found elsewhere in this chapter.

**Mode** User Exec and Global Configuration

**Usage notes** If no additional parameters are specified, then the command output will apply a default selection of parameters shown below:

| Parameter | Description                                                                                  |
|-----------|----------------------------------------------------------------------------------------------|
| direction | Sets debug to packet received, transmitted, or both                                          |
| rx        | packets received by this node                                                                |
| tx        | Packets sent from this node                                                                  |
| 1         | AMF Packet Control header Information, Packet Sequence Number. Enter 1 to select this level. |
| 2         | AMF Detailed Packet Information. Enter 2 to select this level.                               |
| 3         | AMF Packet HEX dump. Enter 3 to select this level.                                           |
| timeout   | Sets the execution timeout for packet logging                                                |

| Parameter  | Description                                                                                       |
|------------|---------------------------------------------------------------------------------------------------|
| <seconds>  | Seconds                                                                                           |
| num-pkts   | Sets the number of packets to be dumped                                                           |
| <quantity> | The actual number of packets                                                                      |
| filter     | Sets debug to filter packets                                                                      |
| node       | Sets the filter on packets for a particular Node                                                  |
| <name>     | The name of the remote node                                                                       |
| interface  | Sets the filter to dump packets from an interface (portx.x.x) on the local node                   |
| <ifname>   | Interface port or virtual-link                                                                    |
| pkt-type   | Sets the filter on packets with a particular AMF packet type                                      |
| 1          | Crosslink Hello BPDU packet with crosslink links information. Enter 1 to select this packet type. |
| 2          | Crosslink Hello BPDU packet with downlink domain information. Enter 2 to select this packet type. |
| 3          | Crosslink Hello BPDU packet with uplink information. Enter 3 to select this packet type.          |
| 4          | Downlink and uplink hello BPDU packets. Enter 4 to select this packet type.                       |
| 5          | Non broadcast hello unicast packets. Enter 5 to select this packet type.                          |
| 6          | Stack hello unicast packets. Enter 6 to select this packet type.                                  |
| 7          | Database description. Enter 7 to select this packet type.                                         |
| 8          | DBE request. Enter 8 to select this packet type.                                                  |
| 9          | DBE update. Enter 9 to select this packet type.                                                   |
| 10         | DBE bitmap update. Enter 10 to select this packet type.                                           |
| 11         | DBE acknowledgment. Enter 11 to select this packet type.                                          |
| 12         | Area Hello Packets. Enter 12 to select this packet type.                                          |
| 13         | Gateway Hello Packets. Enter 13 to select this packet type.                                       |

**Examples** To set a packet debug on node 1 with level 1 and no timeout, use the command:

```
node_1# debug atmf packet direction tx timeout 0
```

To set a packet debug with level 3 and filter packets received from AMF node 1:

```
node_1# debug atmf packet direction tx level 3 filter node_1
```

To enable send and receive 500 packets only on vlink1 for packet types 1, 7, and 11, use the command:

```
node_1# debug atmf packet num-pkts 500 filter interface vlink1
pkt-type 1 7 11
```

This example applies the **debug atmf packet** command and combines many of its options:

```
node_1# debug atmf packet direction rx level 1 num-pkts 60
filter node x930 interface port1.0.1 pkt-type 4 7 10
```



# delete (amf-provision)

**Overview** This command deletes files that have been created for loading onto a provisioned node. It can only be run on master nodes.

**Syntax** delete

**Mode** AMF Provisioning

**Usage notes** This command is only available on master nodes in the AMF network. The command will only work if the provisioned node specified in the command has already been set up (although the device itself is still yet to be installed). Otherwise, an error message is shown when the command is run.

You may want to use the **delete** command to delete a provisioned node that was created in error or that is no longer needed.

This command cannot be used to delete backups created by the AMF backup procedure. In this case, use the command [atmf backup delete](#) to delete the files.

**NOTE:** This command allows provisioned entries to be deleted even if they have been referenced by the [atmf provision \(interface\)](#) command, so take care to only delete unwanted entries.

**Example** To delete backup files for a provisioned node named device3 use the command:

```
device1# atmf provision node device3
device1(atmf-provision)# delete
```

To confirm that the backup files for provisioned node device3 have been deleted use the command:

```
device1# show atmf backup
```

The output should show that the provisioned node device3 no longer exists in the backup file, as shown in the figure below:

Figure 42-7: Sample output showing the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup Enabled
 Schedule 1 per day starting at 03:00
 Next Backup Time 01 Oct 2016 03:00
Backup Bandwidth Unlimited
Backup Media USB (Total 7446.0MB, Free 7297.0MB)
Server Config
 Synchronization Unsynchronized
 Last Run -
 1 Unconfigured
 2 Unconfigured
Current Action Idle
 Started -
 Current Node -

Node Name Date Time In ATMF On Media Status

device1 30 Sep 2016 00:05:49 No Yes Good
device2 30 Sep 2016 00:05:44 Yes Yes Good
```

**Related  
commands**

[atmf provision \(interface\)](#)  
[atmf provision node](#)  
[clone \(amf-provision\)](#)  
[configure boot config \(amf-provision\)](#)  
[configure boot system \(amf-provision\)](#)  
[create \(amf-provision\)](#)  
[identity \(amf-provision\)](#)  
[license-cert \(amf-provision\)](#)  
[locate \(amf-provision\)](#)  
[show atmf provision nodes](#)

**Command  
changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# discovery

**Overview** Use this command to specify how AMF learns about guest nodes.

AMF nodes gather information about guest nodes by using one of the internally defined discovery methods: dynamic, static, or agent.

**Dynamic** learning (the default method) means that AMF learns the guest's IP and MAC addresses from LLDP or DHCP snooping. Dynamic learning is only supported when using IPv4. For IPv6, use static learning.

**Static** learning uses the [switchport atmfguestlink](#) command to specify the guest class name and IP address of the guest node attached to each individual switch port. AMF then learns the MAC addresses of each of the guests of that class from ARP or Neighbor discovery tables.

If you are using the static method, ensure that you have configured the appropriate class type for each of your statically discovered guest nodes.

**Agent** learning uses the AMF agent to retrieve the guest's IP and MAC address. It is only available on guest nodes that support ATMF agent, such as TQ5403 series access points. For step-by-step instructions on using agent discovery for auto-recovery of an TQ5403 series AP, see the [AMF Feature Overview and Configuration Guide](#).

The **no** variant of this command returns the discovery method to **dynamic**.

**Syntax** `discovery [dynamic|static|agent]`  
`no discovery`

| Parameter | Description                          |
|-----------|--------------------------------------|
| dynamic   | Learned from DCHCP Snooping or LLDP. |
| static    | Statically assigned.                 |
| agent     | Learned from the AMF agent.          |

**Default** Dynamic

**Mode** AMF Guest Configuration

**Usage notes** This command is one of several modal commands that are configured and applied for a specific guest-class (mode). Its settings are automatically applied to a guest-node link by the [switchport atmfguestlink](#) command.

**NOTE:** AMF guest nodes are not supported on ports using the OpenFlow protocol.

**Example 1** To configure static discovery for the guest-class 'camera', use the following commands:

```
Node1# configure terminal
Node1(config)# atmf guest-class camera
Node1(config-atmf-guest)# discovery static
```

**Example 2** To return the discovery method for the guest class TQ6602 to its default of **dynamic**, use the following commands:

```
Node1# configure terminal
Node1(config)# atmf guest-class TQ6602
Node1(config-atmf-guest)# no discovery
```

**Related commands**

- [atmf guest-class](#)
- [switchport atmf-guestlink](#)
- [show atmf links guest](#)
- [show atmf nodes](#)

**Command changes** Version 5.5.3-0.1: **agent** parameter added

# description (amf-container)

**Overview** Use this command to set the description on an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove the description from an AMF container.

**Syntax** `description <description>`  
`no description`

| Parameter                        | Description                                                      |
|----------------------------------|------------------------------------------------------------------|
| <code>&lt;description&gt;</code> | Enter up to 128 characters of text describing the AMF container. |

**Mode** AMF Container Configuration

**Example** To set the description for AMF container “vac-wlg-1” to “Wellington area”, use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# description Wellington area
```

To remove the description for AMF container “vac-wlg-1”, use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# no description
```

**Related commands** [atmf container](#)  
[show atmf container](#)

**Command changes** Version 5.4.7-0.1: command added

# erase factory-default

**Overview** This command erases all data from NVS and all data from flash **except** the following:

- the boot release file (a .rel file) and its release setting file
- all license files
- the latest GUI release file

The device is then rebooted and returned to its factory default condition. The device can then be used for AMF automatic node recovery.

**Syntax** `erase factory-default`

**Mode** Privileged Exec

**Usage notes** This command is an alias to the [atmf cleanup](#) command.

**Example** To erase data, use the command:

```
Node_1# erase factory-default
```

```
This command will erase all NVS, all flash contents except for
the boot release, a GUI resource file, and any license files,
and then reboot the switch. Continue? (y/n):y
```

**Related commands** [atmf cleanup](#)

# firmware-url

**Overview** Use this command to specify the location of an AP guest node's firmware file when preparing the AP for auto-recovery. AMF cannot back up AP firmware files (only configuration files), so you need to store the firmware file somewhere accessible and use this command to provide the AlliedWare Plus device with the file's location.

For step-by-step instructions for auto-recovery of an TQ5403 series AP, see the [AMF Feature Overview and Configuration Guide](#).

Use the **no** variant of this command to remove the URL.

**Syntax** `firmware-url <name>`  
`no firmware-url`

| Parameter                 | Description                                                                                                                                                                                                                                                   |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;name&gt;</code> | The file's directory or filename. We recommend specifying a directory because that makes it easier to keep the firmware file up to date. The following protocols are supported: http, https, tftp, usb, and card. Do not change the firmware file's filename. |

**Default** No URL is configured

**Mode** AMF Guest Configuration

**Example** To specify, on a device named node2, that the firmware file for a TQ5403 AP is stored in the top level of a USB stick, use the commands:

```
node2# configure terminal
node2(config)# atmf guest-class TQ5403
node2(config-guest)# firmware-url usb:
```

To specify, on a device named node2, that the firmware file for a TQ5403 AP is stored on a TFTP server with an address of 192.168.2.1, use the commands:

```
node2# configure terminal
node2(config)# atmf guest-class TQ5403
node2(config-guest)# firmware-url tftp://192.168.2.1/
```

**Related commands**

- [atmf guest-class](#)
- [discovery](#)
- [login-fallback enable](#)
- [modeltype](#)
- [show atmf guests](#)
- [show atmf guests detail](#)

switchport atmf-guestlink

**Command changes** Version 5.5.3-0.1: command added



# http-enable

**Overview** This command is used to enable GUI access to a guest node. When **http-enable** is configured, the port number is set to its default of 80. If the guest node is using a different port for HTTP, you can configure this using the **port** parameter.

This command is used to inform the GUI that this device has an HTTP interface at the specified port number so that a suitable URL can be provided to the user.

Use the **no** variant of this command to disable HTTP.

**Syntax** `http-enable [port <port-number>]`  
`no http-enable`

| Parameter     | Description                       |
|---------------|-----------------------------------|
| port          | TCP port number.                  |
| <port-number> | The port number to be configured. |

**Default** Not set

**Mode** AMF Guest Configuration

**Usage notes** If **http-enable** is selected without a **port** parameter the port number will default to 80.

**Example** To enable HTTP access to a guest node on port 80 (the default), use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class Camera
node1(config-atmf-guest)# http-enable
```

To enable HTTP access to a guest node on port 400, use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class Camera
node1(config-atmf-guest)# http-enable port 400
```

To disable HTTP access to a guest node, use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class Camera
node1(config-atmf-guest)# no http-enable
```

**Related commands** [atmf guest-class](#)  
[switchport atmf-guestlink](#)  
[show atmf links guest](#)

`show atmf nodes`

# identity (amf-provision)

**Overview** Use this command to create an identity token for provisioning an isolated AMF node. An isolated node is an AMF member that is only connected to the rest of the AMF network via a virtual-link.

This command allows these nodes, which have no AMF neighbors, to be identified for provisioning purposes. They are identified using an identity token which is based on either the next-hop MAC address of the provisioned node, or the serial number of the device being provisioned. This identity token is stored on the AMF master.

Use the **no** variant of this command to remove the identity token for a node.

**Syntax**

```
identity mac-address <mac-address> prefix
<ip-address/prefix-length>

identity serial-number <serial-number> prefix
<ip-address/prefix-length>

no identity
```

| Parameter                      | Description                                                                                 |
|--------------------------------|---------------------------------------------------------------------------------------------|
| mac-address                    | Specify the next-hop MAC address of the device being provisioned.                           |
| <mac-address>                  | MAC address of the port the provisioned node is connected to, in the format xxxx.xxxx.xxxx. |
| serial-number                  | Specify the serial number of the device to be provisioned.                                  |
| <serial-number>                | Serial number of the device that is being provisioned.                                      |
| prefix                         | IPv4 address, and prefix length, of the virtual-link interface on the isolated node         |
| <ip-address/<br>prefix-length> | IPv4 address, and prefix length, in A.B.C.D/M format.                                       |

**Mode** AMF Provisioning

**Usage notes** To provision an isolated node, first create a configuration for the node using the [create \(amf-provision\)](#) and/or the [clone \(amf-provision\)](#) commands.

Then create an identity token for the provisioned node by either specifying its next-hop MAC address or by specifying the serial number of the replacement device. The advantage of using the next-hop MAC address is that any device, regardless of its serial number, can be added to the network but using the serial number maybe preferred in situations where the next-hop MAC address is not easy to obtain.

The [atmf recovery-server](#) option must be enabled on the AMF master before attempting to provision the device. This option allows the AMF master to process recovery requests from isolated AMF nodes.

See the [AMF Feature Overview and Configuration Guide](#) for information on preparing your network for recovering or provisioning isolated nodes.

**Example** To create an identity token on your AMF master for a device named “my-x930” with serial number “A10064A172100008”, use the command:

```
awplus# atmf provision node my-x930

awplus(atmf-provision)# identity serial-number
A10064A172100008 prefix 192.168.2.25/24
```

To create an identity token on your AMF master for a device named “my-x930” with next-hop MAC address “0000.cd28.0880”, use the command:

```
awplus# atmf provision node my-x930

awplus(atmf-provision)# identity mac-address 0000.cd28.0880
prefix 192.168.2.25/24
```

To delete the identity token from your AMF master for a device named “my-x930”, use the command:

```
awplus# atmf provision node my-x930

awplus(atmf-provision)# no identity
```

**Related  
commands**

[atmf cleanup](#)  
[atmf provision \(interface\)](#)  
[atmf provision node](#)  
[atmf recovery-server](#)  
[atmf virtual-link](#)  
[clone \(amf-provision\)](#)  
[configure boot config \(amf-provision\)](#)  
[configure boot system \(amf-provision\)](#)  
[create \(amf-provision\)](#)  
[delete \(amf-provision\)](#)  
[license-cert \(amf-provision\)](#)  
[locate \(amf-provision\)](#)  
[show atmf provision nodes](#)

**Command  
changes**

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode  
Version 5.4.7-2.1: command added

# license-cert (amf-provision)

**Overview** This command is used to set up the license certificate for a provisioned node.

The certificate file usually has all the license details for the network, and can be stored anywhere in the network. This command makes a hidden copy of the certificate file and stores it in the space set up for the provisioned node on AMF backup media.

For node provisioning, the new device has not yet been part of the AMF network, so the user is unlikely to know its product ID or its MAC address. When such a device joins the network, assuming that this command has been applied successfully, the copy of the certificate file will be applied automatically to the provisioned node.

Once the new device has been resurrected on the network and the certificate file has been downloaded to the provisioned node, the hidden copy of the certificate file is deleted from AMF backup media.

Use the **no** variant of this command to set it back to the default.

This command can only be run on AMF master nodes.

**Syntax** `license-cert <file-path|URL>`  
`no license-cert`

| Parameter                          | Description                                                                   |
|------------------------------------|-------------------------------------------------------------------------------|
| <code>&lt;file-path URL&gt;</code> | The name of the certificate file. This can include the file-path of the file. |

**Default** No license certificate file is specified for the provisioned node.

**Mode** AMF Provisioning

**Usage notes** This command is only available on master nodes in the AMF network. It will only operate if the provisioned node specified in the command has already been set up, and if the license certification is present in the backup file. Otherwise, an error message is shown when the command is run.

**Example 1** To apply the license certificate 'cert1.txt' stored on a TFTP server for AMF provisioned node "device2", use the command:

```
device1# atmf provision node device2
device1(atmf-provision)# license-cert
tftp://192.168.1.1/cert1.txt
```

**Example 2** To apply the license certificate 'cert2.txt' stored in the AMF master's flash directory for AMF provisioned node 'host2', use the command:

```
device1# atmf provision node host2
device1(atmf-provision)# license-cert /cert2.txt
```

To confirm that the license certificate has been applied to the provisioned node, use the command [show atmf provision nodes](#). The output from this command is shown below, and displays license certification details in the last line.

Figure 42-8: Sample output from the **show atmf provision nodes** command

```
device1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media: SD (Total 3827.0MB, Free 3481.1MB)

Node Name : device2
Date & Time : 06-Oct-2016 & 23:25:44
Provision Path : card:/atmf/nodes

Boot configuration :
Current boot image : x510-5.4.6-1.4.rel (file exists)
Backup boot image : x510-5.4.6-1.3.rel (file exists)
Default boot config : flash:/default.cfg (file exists)
Current boot config : flash:/abc.cfg (file exists)
Backup boot config : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file : ../configs/.sw_v2.lic
 : ../configs/.swfeature.lic
Certificate file : card:/atmf/lok/nodes/awplus1/flash/.atmf-lic-cert
```

**Related commands**

- [atmf provision \(interface\)](#)
- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [configure boot config \(amf-provision\)](#)
- [configure boot system \(amf-provision\)](#)
- [create \(amf-provision\)](#)
- [delete \(amf-provision\)](#)
- [identity \(amf-provision\)](#)
- [locate \(amf-provision\)](#)
- [show atmf provision nodes](#)

**Command changes** Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

# locate (amf-provision)

**Overview** This command changes the present working directory to the directory of a provisioned node. This makes it easier to edit files and create a unique provisioned node in the backup.

This command can only be run on AMF master nodes.

**NOTE:** We advise that after running this command, you return to a known working directory, typically flash.

**Syntax** locate

**Mode** AMF Provisioning

**Example** To change the working directory that happens to be on device1 to the directory of provisioned node device2, use the following command:

```
device1# atmf provision node device2
device1[atmf-provision]# locate
```

The directory of the node device2 should now be the working directory. You can use the command `pwd` to check this, as shown in the following figure.

Figure 42-9: Sample output from the `pwd` command

```
device2#pwd
card:/atmf/building_2/nodes/device2/flash
```

The output above shows that the working directory is now the flash of device2.

**Related commands**

- [atmf provision \(interface\)](#)
- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [configure boot config \(amf-provision\)](#)
- [configure boot system \(amf-provision\)](#)
- [copy \(amf-provision\)](#)
- [create \(amf-provision\)](#)
- [delete \(amf-provision\)](#)
- [identity \(amf-provision\)](#)
- [license-cert \(amf-provision\)](#)
- [locate \(amf-provision\)](#)
- [pwd](#)
- [show atmf provision nodes](#)

**Command changes** Version 5.4.9-0.1: syntax change due to new AMF provisioning mode



# log event-host

**Overview** Use this command to set up an external host to log AMF topology events through Vista Manager. This command is run on the Master device.

Use the **no** variant of this command to disable log events through Vista Manager.

**Syntax** `log event-host [<ipv4-addr>|<ipv6-addr>] atmf-topology-event`  
`no log event-host [<ipv4-addr>|<ipv6-addr>] atmf-topology-event`

| Parameter   | Description                    |
|-------------|--------------------------------|
| <ipv4-addr> | ipv4 address of the event host |
| <ipv6-addr> | ipv6 address of the event host |

**Default** Log events are disabled by default.

**Mode** Global Configuration

**Usage notes** Event hosts are set so syslog sends the messages out as they come.  
Note that there is a difference between log event and log host messages:

- Log event messages are sent out as they come by syslog
- Log host messages are set to wait for a number of messages (20) to send them out together for traffic optimization.

**Example** To enable Node 1 to log event messages from host IP address 192.0.2.31, use the following commands:

```
Node1# configure terminal
```

```
Node1(config)# log event-host 192.0.2.31 atmf-topology-event
```

To disable Node 1 to log event messages from host IP address 192.0.2.31, use the following commands:

```
Node1# configure terminal
```

```
Node1(config)# no log event-host 192.0.2.31 atmf-topology-event
```

**Related commands** [atmf topology-gui enable](#)

# login-fallback enable

**Overview** Use this command to enable login fallback on TQ model AMF guest nodes. This allows AMF to try the factory default username and password if the guest node's saved username and password fail.

Use the **no** variant of this command to disable login fallback.

**Syntax** login-fallback enable  
no login-fallback enable

**Default** Disabled

**Mode** AMF Guest Configuration

**Usage notes** This feature is only supported on TQ model guest nodes.

Login fallback means: if a guest node's saved username and password fail, AMF will try to connect to the node using the factory default username and password (manager/friend). When a new TQ replaces an existing TQ, this allows the new TQ to be discovered and managed as an AMF guest node. AMF can then start the AMF guest node recovery procedure.

**Example** To use the login fallback feature, first create an AMF guest class for TQ model APs. Then enable the login fall back feature.

For example, to enable login fallback on the guest-class AT-TQ5k, use the commands:

```
node1#configuration terminal
node1(config)#atmf guest-class AT-TQ5k
node1(config-atmf-guest)#login-fallback enable
node1(config-atmf-guest)#end
node1#
```

**Related commands** [atmf guest-class](#)  
[modeltype](#)  
[switchport atmf-guestlink](#)  
[show atmf links guest](#)

**Command changes** Version 5.5.0-1.1: command added

# modeltype

**Overview** This command sets the expected model type of the guest node. The model type will default to **other** if nothing is set.

Use the **no** variant of this command to reset the model type to **other**.

**Syntax** `modeltype {alliedware|aw+|onvif|tq|other}`  
`no modeltype`

| Parameter  | Description                                                  |
|------------|--------------------------------------------------------------|
| alliedware | A legacy Allied Telesis operating system.                    |
| aw+        | The Allied Telesis AlliedWare Plus operating system.         |
| onvif      | ONVIF (Open Network Video Interface Forum) Profile Q devices |
| tq         | An Allied Telesis TQ Series wireless access point.           |
| other      | Used where the model type is outside the above definitions.  |

**Default** Default to **other**

**Mode** AMF Guest Configuration

**Examples** To assign the model type **tq** to the guest-class called 'tq\_device', use the commands:

```
node1# configure terminal
node1(config)# atmf guest-class tq_device
node1(config-vmf-guest)# modeltype tq
```

To remove the model type **tq** from the guest-class called 'tq\_device', and reset it to the default of **other**, use the commands:

```
node1# configure terminal
node1(config)# atmf guest-class tq_device
node1(config-vmf-guest)# no modeltype
```

**Related commands** [vmf guest-class](#)  
[switchport vmf-guestlink](#)  
[show vmf links guest](#)

**Command changes** Version 5.4.9-2.1: **onvif** parameter added

# service atmf-application-proxy

**Overview** Use this command to enable the AMF Application Proxy service. This service distributes messages across all AMF nodes.

Currently this is used for threat protection. When an AMF Security (AMF-Sec) Controller detects a threat, it issues a request to block the address the threat originated from. The AMF Application Proxy service distributes this message to all AMF nodes. An AMF master accepts this block request and instructs the subordinate AMF node to block the relevant device.

Use the **no** variant of this command to disable the AMF Application Proxy service.

**Syntax** `service atmf-application-proxy`  
`no service atmf-application-proxy`

**Default** The AMF Application Proxy service is disabled by default.

**Mode** Global Configuration

**Usage notes** The AMF master maintains a list of all threats and will send this list to any AMF node, or VCS member, when it boots and joins the AMF network.

In order for this to work the follow must be configured:

- the AMF Application Proxy service on all AMF nodes that need to receive the messages.
- the Hypertext Transfer Protocol (HTTP) service on all nodes that are running the AMF Application Proxy service (see [service http](#)).

**Example** To enable the AMF Application Proxy service, use the commands

```
awplus# configure terminal
awplus(config)# service atmf-application-proxy
```

To disable the AMF Application Proxy service, use the commands

```
awplus# configure terminal
awplus(config)# no service atmf-application-proxy
```

**Related commands** [application-proxy threat-protection](#)  
[application-proxy whitelist server](#)  
[clear application-proxy threat-protection](#)  
[show application-proxy threat-protection](#)

**Command changes** Version 5.4.7-2.2: command added

# show application-proxy threat-protection

**Overview** Use this command to list all the IP addresses blocked by the AMF Application Proxy service. It also shows the global threat-detection configuration.

**Syntax** `show application-proxy threat-protection [all]`

| Parameter | Description                               |
|-----------|-------------------------------------------|
| all       | Include information for non-local blocks. |

**Mode** Privileged Exec

**Example** To list the addresses blocked by the AMF Application Proxy service, use the command:

```
awplus# show application-proxy threat-protection
```

**Output** Figure 42-10: Example output from **show application-proxy threat-protection**

|                                                 |           |                |                         |           |
|-------------------------------------------------|-----------|----------------|-------------------------|-----------|
| awplus#show application-proxy threat-protection |           |                |                         |           |
| Quarantine Vlan                                 |           | :              | vlan200                 |           |
| Global IP-Filter                                |           | :              | Enabled                 |           |
| IP-Filter Limit Exceeded                        |           | :              | 0                       |           |
| Redirect-URL                                    |           | :              | http://my.dom/help.html |           |
| Client IP                                       | Interface | MAC Address    | VLAN                    | Action    |
| -----                                           |           |                |                         |           |
| 10.34.199.110                                   | -         | -              | -                       | link-down |
| 10.34.199.116                                   | port1.0.3 | 001a.eb93.ec5d | 1                       | drop      |
| 10.1.179.1                                      | *         | *              | *                       | ip-filter |
| ...                                             |           |                |                         |           |

Table 42-1: Parameters in the output from **show application-proxy threat-protection**

| Parameter                | Description                                                                  |
|--------------------------|------------------------------------------------------------------------------|
| Quarantine Vlan          | The name of the quarantine VLAN.                                             |
| Global IP-Filter         | The status of global IP filtering.                                           |
| IP-Filter Limit Exceeded | The number of times an ACL failed to be installed due to insufficient space. |
| Redirect-URL             | The URL a blocked user is redirected to.                                     |

**Related commands** [application-proxy quarantine-vlan](#)  
[application-proxy threat-protection](#)

clear application-proxy threat-protection  
service atmf-application-proxy

**Command changes** Version 5.4.7-2.2: command added

# show application-proxy whitelist advertised-address

**Overview** Use this command to show the Layer 3 interface and its IPv4 address that is advertised as the application-proxy whitelist address.

**Syntax** `show application-proxy whitelist advertised-address`

**Mode** Privileged Exec

**Example** To display the interface and IPv4 address advertised as the application-proxy whitelist address, use the command:

```
awplus# show application-proxy whitelist advertised-address
```

**Output** Figure 42-11: Example output from **show application-proxy whitelist advertised-address**

```
awplus#show application-proxy whitelist advertised-address
ATMF Application Proxy Whitelist advertised-address:
 Interface : vlan1001
 IP address : 10.34.16.5
```

**Related commands** [application-proxy whitelist advertised-address](#)  
[application-proxy whitelist server](#)

**Command changes** Version 5.4.9-1.1: command added

# show application-proxy whitelist interface

**Overview** Use this command to display the status of port authentication on the specified interface.

**Syntax** `show application-proxy whitelist interface [<interface-list>]`

| Parameter                           | Description                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;interface-list&gt;</code> | The interfaces or ports to display information about. An interface-list can be: <ul style="list-style-type: none"><li>• a switchport (e.g. port1.0.4)</li><li>• a continuous range of ports separated by a hyphen (e.g. port1.0.1-1.0.4)</li><li>• a comma-separated list (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list.</li></ul> The specified interface must exist. |

**Mode** Privileged Exec

**Example** To display the port authentication information for all interfaces, use the command:

```
awplus# show application-proxy whitelist interface
```

To display the port authentication information for port1.0.4, use the command

```
awplus# show application-proxy whitelist interface port1.0.4
```



**Output** Figure 42-12: Example output from **show application-proxy whitelist interface**

```
awplus#sh application-proxy whitelist interface
Authentication Info for interface port1.0.1
 portEnabled: false - portControl: Auto
 portStatus: Unknown
 reAuthenticate: disabled
 reAuthPeriod: 3600
 PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
 PAE: connectTimeout: 30
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in
 KT: keyTxEnabled: false
 critical: disabled
 guestVlan: disabled
 guestVlanForwarding:
 none
 authFailVlan: disabled
 dynamicVlanCreation: disabled
 multiVlanSession: disabled
 hostMode: single-host
 dot1x: disabled
 authMac: enabled
 method: PAP
 scheme: mac
 reauthRelearning: disabled
 authWeb: disabled
 twoStepAuthentication:
 configured: disabled
 actual: disabled
 supplicantMac: none
 supplicantIpv4: none
Authentication Info for interface port1.0.2
...
```

**Related commands**

- [application-proxy whitelist enable](#)
- [application-proxy whitelist server](#)
- [show application-proxy whitelist server](#)
- [show application-proxy whitelist supplicant](#)

**Command changes** Version 5.4.9-0.1: command added

# show application-proxy whitelist server

**Overview** Use this command to display the external RADIUS server details for the application-proxy whitelist feature.

**Syntax** `show application-proxy whitelist server`

**Mode** Privileged Exec

**Example** To display the external RADIUS server details for the application-proxy whitelist feature, use the command:

```
awplus# show application-proxy whitelist server
```

**Output** Figure 42-13: Example output from **show application-proxy whitelist server**

```
awplus#show application-proxy whitelist server

Application Proxy Whitelist Details:

External Server Details:
 IP: 192.168.1.10
 Port: 2083
 Protection: TLS
 Trustpoint: None (Authentication disabled)

Proxy Details:
 IP: 172.31.0.5
 Status: Alive
```

**Related commands**

- [application-proxy whitelist enable](#)
- [application-proxy whitelist server](#)
- [show application-proxy whitelist interface](#)
- [show application-proxy whitelist supplicant](#)

**Command changes** Version 5.4.9-0.1: command added

# show application-proxy whitelist supplicant

**Overview** Use this command to display the current configuration and status for each supplicant attached to an application-proxy whitelist port.

**Syntax** `show application-proxy whitelist supplicant [interface <interface-list>|<mac-addr>|brief]`

| Parameter                     | Description                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface<br><interface-list> | The interfaces or ports to display information about. An interface-list can be: <ul style="list-style-type: none"><li>• a switchport (e.g. port1.0.4)</li><li>• a continuous range of ports separated by a hyphen (e.g. port1.0.1-1.0.4)</li><li>• a comma-separated list (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list.</li></ul> The specified interface must exist. |
| <mac-addr>                    | MAC (hardware) address of the supplicant. Entry format is HHHH.HHHH.HHHH (hexadecimal)                                                                                                                                                                                                                                                                                                            |
| brief                         | Brief summary of the supplicant state.                                                                                                                                                                                                                                                                                                                                                            |

**Mode** Privileged Exec

**Example** To display the supplicant information for all ports, use the command:

```
awplus# show application-proxy whitelist supplicant
```

To display the supplicant information for port1.0.4, use the command:

```
awplus# show application-proxy whitelist supplicant interface
port1.0.4
```

**Output** Figure 42-14: Example output from **show application-proxy whitelist supplicant**

```
awplus#show application-proxy whitelist supplicant
Interface port1.0.4
 authenticationMethod: dot1x/mac/web
 Two-Step Authentication
 firstMethod: mac
 secondMethod: dot1x/web
 totalSupplicantNum: 1
 authorizedSupplicantNum: 1
 macBasedAuthenticationSupplicantNum: 0
 dot1xAuthenticationSupplicantNum: 0
 webBasedAuthenticationSupplicantNum: 1
 otherAuthenticationSupplicantNum: 0

 Supplicant name: test
 Supplicant address: 001c.233e.e15a
 authenticationMethod: WEB-based Authentication
 Two-Step Authentication:
 firstAuthentication: Pass - Method: mac
 secondAuthentication: Pass - Method: web
 portStatus: Authorized - currentId: 1
 abort:F fail:F start:F timeout:F success:T
 PAE: state: Authenticated - portMode: Auto
 PAE: reAuthCount: 0 - rxRespId: 0
 PAE: quietPeriod: 60 - maxReauthReq: 2
 BE: state: Idle - reqCount: 0 - idFromServer: 0
 CD: adminControlledDirections: in operControlledDirections: in
 CD: bridgeDetected: false
 KR: rxKey: false
 KT: keyAvailable: false - keyTxEnabled: false
 RADIUS server group (auth): radius
 RADIUS server (auth): 192.168.1.40
...
```

**Related commands**

- [application-proxy whitelist enable](#)
- [application-proxy whitelist server](#)
- [show application-proxy whitelist interface](#)
- [show application-proxy whitelist server](#)

**Command changes** Version 5.4.9-0.1: command added

# show atmf

**Overview** Displays information about the current AMF node.

**Syntax** `show atmf [summary|tech|nodes|session]`

| Parameter | Description                                               |
|-----------|-----------------------------------------------------------|
| summary   | Displays summary information about the current AMF node.  |
| tech      | Displays global AMF information.                          |
| nodes     | Displays a list of AMF nodes together with brief details. |
| session   | Displays information on an AMF session.                   |

**Default** Only summary information is displayed.

**Mode** User Exec and Privileged Exec

**Usage notes** AMF uses internal VLANs to communicate between nodes about the state of the AMF network. Two VLANs have been selected specifically for this purpose. Once these have been assigned, they are reserved for AMF and cannot be used for other purposes

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Example 1** To show summary information on AMF node\_1 use the following command:

```
node_1# show atmf summary
```

**Table 43:** Output from the **show atmf summary** command

|                           |                |
|---------------------------|----------------|
| node_1#show atmf summary  |                |
| ATMF Summary Information: |                |
| ATMF Status               | : Enabled      |
| Network Name              | : Test_network |
| Node Name                 | : node_1       |
| Role                      | : Master       |
| Restricted login          | : Disabled     |
| Current ATMF Nodes        | : 3            |

**Example 2** To show information specific to AMF nodes use the following command:

```
node_1# show atmf nodes
```

**Example 3** The **show amf session** command displays all CLI (Command Line Interface) sessions for users that are currently logged in and running a CLI session.

To display AMF active sessions, use the following command:

```
node_1# show atmf session
```

For example, in the output below, node\_1 and node\_5 have active users logged in.

**Table 44:** Output from the **show atmf session** command

|                                      |                  |
|--------------------------------------|------------------|
| node_1#show atmf session             |                  |
| CLI Session Neighbors                |                  |
| Session ID                           | : 73518          |
| Node Name                            | : node_1         |
| PID                                  | : 7982           |
| Link type                            | : Broadcast-cli  |
| MAC Address                          | : 0000.0000.0000 |
| Options                              | : 0              |
| Our bits                             | : 0              |
| Link State                           | : Full           |
| Domain Controller                    | : 0              |
| Backup Domain Controller             | : 0              |
| Database Description Sequence Number | : 00000000       |
| First Adjacency                      | : 1              |
| Number Events                        | : 0              |
| DBE Retransmit Queue Length          | : 0              |
| DBE Request List Length              | : 0              |
| Session ID                           | : 410804         |
| Node Name                            | : node_5         |
| PID                                  | : 17588          |
| Link type                            | : Broadcast-cli  |
| MAC Address                          | : 001a.eb56.9020 |
| Options                              | : 0              |
| Our bits                             | : 0              |
| Link State                           | : Full           |
| Domain Controller                    | : 0              |
| Backup Domain Controller             | : 0              |
| Database Description Sequence Number | : 00000000       |
| First Adjacency                      | : 1              |
| Number Events                        | : 0              |
| DBE Retransmit Queue Length          | : 0              |
| DBE Request List Length              | : 0              |

**Example 4** The AMF tech command collects all the AMF commands, and displays them. You can use this command when you want to see an overview of the AMF network.

To display AMF technical information, use the following command:

```
node_1# show atmf tech
```

**Table 45:** Output from the **show atmf tech** command

```

node_1#show atmf tech
ATMF Summary Information:

ATMF Status : Enabled
Network Name : ATMF_NET
Node Name : node_1
Role : Master
Current ATMF Nodes : 8

ATMF Technical information:

Network Name : ATMF_NET
Domain : node_1's domain
Node Depth : 0
Domain Flags : 0
Authentication Type : 0
MAC Address : 0014.2299.137d
Board ID : 287
Domain State : DomainController
Domain Controller : node_1
Backup Domain Controller : node2
Domain controller MAC : 0014.2299.137d
Parent Domain : -
Parent Domain Controller : -
Parent Domain Controller MAC : 0000.0000.0000
Number of Domain Events : 0
Crosslink Ports Blocking : 0
Uplink Ports Waiting on Sync : 0
Crosslink Sequence Number : 7
Domains Sequence Number : 28
Uplink Sequence Number : 2
Number of Crosslink Ports : 1
Number of Domain Nodes : 2
Number of Neighbors : 5
Number of Non Broadcast Neighbors : 3
Number of Link State Entries : 1
Number of Up Uplinks : 0
Number of Up Uplinks on This Node : 0
DBE Checksum : 84fc6
Number of DBE Entries : 0
Management Domain Ifindex : 4391
Management Domain VLAN : 4091
Management ifindex : 4392
Management VLAN : 4092

```

**Table 46:** Parameter definitions from the **show atmf tech** command

| Parameter    | Definition                                         |
|--------------|----------------------------------------------------|
| ATMF Status  | The Node's AMF status, either Enabled or Disabled. |
| Network Name | The AMF network that a particular node belongs to. |

**Table 46:** Parameter definitions from the **show atmf tech** command (cont.)

| Parameter          | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Node Name          | The name assigned to a particular node.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Role               | The role configured for this AMF device, either Master or Member.                                                                                                                                                                                                                                                                                                                                                                                        |
| Current ATMF Nodes | The count of AMF nodes in an AMF Network.                                                                                                                                                                                                                                                                                                                                                                                                                |
| Node Address       | An address used to access a remotely located node (.atmf).                                                                                                                                                                                                                                                                                                                                                                                               |
| Node ID            | A unique identifier assigned to a Node on an AMF network.                                                                                                                                                                                                                                                                                                                                                                                                |
| Node Depth         | The number of nodes in path from this node to level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.                                                                                                                                                                                                                                                   |
| Domain State       | The state of Node in a Domain in AMF network as Controller/Backup.                                                                                                                                                                                                                                                                                                                                                                                       |
| Recovery State     | The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.                                                                                                                                                                                                                                                                                                                                   |
| Management VLAN    | The VLAN created for traffic between Nodes of different domain (up/down links). <ul style="list-style-type: none"> <li>VLAN ID - In this example VLAN 4092 is configured as the Management VLAN.</li> <li>Management Subnet - Network prefix for the subnet.</li> <li>Management IP Address - The IP address allocated for this traffic.</li> <li>Management Mask - The subnet mask used to create a subnet for this traffic (255.255.128.0).</li> </ul> |
| Domain VLAN        | The VLAN assigned for traffic between Nodes of same domain (crosslink). <ul style="list-style-type: none"> <li>VLAN ID - In this example VLAN 4091 is configured as the domain VLAN.</li> <li>Domain Subnet. The subnet address used for this traffic.</li> <li>Domain IP Address. The IP address allocated for this traffic.</li> <li>Domain Mask. The subnet mask used to create a subnet for this traffic (255.255.128.0).</li> </ul>                 |
| Device Type        | The Product Series name.                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ATMF Master        | Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not).                                                                                                                                                                                                                                                                                                                                                                 |
| SC                 | The device configuration, one of C - Chassis (SBx8100 Series), S - Stackable (VCS) or N - Standalone.                                                                                                                                                                                                                                                                                                                                                    |
| Parent             | The node to which the current node has an active uplink.                                                                                                                                                                                                                                                                                                                                                                                                 |
| Node Depth         | The number of nodes in the path from this node to the master node.                                                                                                                                                                                                                                                                                                                                                                                       |

**Related commands** [show atmf detail](#)



# show atmf area

**Overview** Use this command to display information about an AMF area. On AMF controllers, this command displays all areas that the controller is aware of. On remote AMF masters, this command displays the controller area and the remote local area. On gateways, this command displays the controller area and remote master area.

**Syntax** `show atmf area [detail] [<area-name>]`

| Parameter   | Description                                                                     |
|-------------|---------------------------------------------------------------------------------|
| detail      | Displays detailed information                                                   |
| <area-name> | Displays information about master and gateway nodes in the specified area only. |

**Mode** Privileged Exec

**Example 1** To show information about all areas, use the command:

```
controller-1# show atmf area
```

The following figure shows example output from running this command on a controller.

**Table 47:** Example output from the **show atmf area** command on a Controller.

| controller-1#show atmf area |         |                  |                |               |            |
|-----------------------------|---------|------------------|----------------|---------------|------------|
| ATMF Area Information:      |         |                  |                |               |            |
| * = Local area              |         |                  |                |               |            |
| Area Name                   | Area ID | Local Gateway    | Remote Gateway | Remote Master | Node Count |
| * NZ                        | 1       | Reachable        | N/A            | N/A           | 3          |
| Wellington                  | 2       | Reachable        | Reachable      | Auth OK       | 120        |
| Canterbury                  | 3       | Reachable        | Reachable      | Auth Error    | -          |
| SiteA-AREA                  | 14      | Unreachable      | Unreachable    | Unreachable   | -          |
| Auckland                    | 100     | Reachable        | Reachable      | Auth Start    | -          |
| Southland                   | 120     | Reachable        | Reachable      | Auth OK       | 54         |
| Area count:                 | 6       | Area node count: |                |               | 177        |

The following figure shows example output from running this command on a remote master.

**Table 48:** Example output from the **show atmf area** command on a remote master.

```
Canterbury#show atmf area

ATMF Area Information:

* = Local area
```

| Area Name    | Area ID | Local Gateway          | Remote Gateway | Remote Master | Node Count |
|--------------|---------|------------------------|----------------|---------------|------------|
| NZ           | 1       | Reachable              | N/A            | N/A           | -          |
| * Canterbury | 3       | Reachable              | N/A            | N/A           | 40         |
| Area count:  | 2       | Local area node count: |                |               | 40         |

**Table 49:** Parameter definitions from the **show atmf area** command

| Parameter       | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| *               | Indicates the area of the device on which the command is being run.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Area Name       | The name of each area.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Area ID         | The ID of the area.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Local Gateway   | Whether the local gateway node is reachable or not.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Remote Gateway  | Whether the remote gateway node is reachable or not. This is one of the following: <ul style="list-style-type: none"> <li>Reachable, if the link has been established.</li> <li>Unreachable, if a link to the remote area has not been established. This could mean that a port or vlan is down, or that inconsistent VLANs have been configured using the <a href="#">switchport atmf-arealink</a> command.</li> <li>N/A for the area of the controller or remote master on which the command is being run, because the gateway node on that device is local.</li> <li>Auth Start, which may indicate that the area names match on the controller and remote master, but the IDs do not match.</li> <li>Auth Error, which indicates that the areas tried to authenticate but there is a problem. For example, the passwords configured on the controller and remote master may not match, or a password may be missing on the remote master.?</li> <li>Auth OK, which indicates that area authentication was successful and you can now use the <a href="#">atmf select-area</a> command.</li> </ul> |
| Remote Master   | Whether the remote master node is reachable or not. This is N/A for the area of the controller or remote master on which the command is being run, because the master node on that device is local.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Node Count      | The number of nodes in the area.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Area Count      | The number of areas controlled by the controller.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Area Node Count | The total number of nodes in the area.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Example 2** To show detailed information about the areas, use the command:

```
controller-1# show atmf area detail
```

The following figure shows example output from running this command.

**Table 50:** Output from the **show atmf area detail** command

|                                    |                      |
|------------------------------------|----------------------|
| controller-1#show atmf area detail |                      |
| ATMF Area Detail Information:      |                      |
| Controller distance                | : 0                  |
| Controller Id                      | : 21                 |
| Backup Available                   | : FALSE              |
| Area Id                            | : 2                  |
| Gateway Node Name                  | : controller-1       |
| Gateway Node Id                    | : 342                |
| Gateway Ifindex                    | : 6013               |
| Masters Count                      | : 1                  |
| Master Node Name                   | : well-master (329)  |
| Node Count                         | : 2                  |
| Area Id                            | : 3                  |
| Gateway Node Name                  | : controller-1       |
| Gateway Node Id                    | : 342                |
| Gateway Ifindex                    | : 4511               |
| Masters Count                      | : 2                  |
| Master Node Name                   | : cant1-master (15)  |
| Master Node Name                   | : cant2-master (454) |
| Node Count                         | : 2                  |

**Related commands**

- [show atmf area summary](#)
- [show atmf area nodes](#)
- [show atmf area nodes-detail](#)

# show atmf area guests

**Overview** This command will display details of all guests that the controller is aware of.

**Syntax** show atmf area guests [<area-name> [<node-name>]]

| Parameter   | Description                                       |
|-------------|---------------------------------------------------|
| <area-name> | The area name for guest information               |
| <node-name> | The name of the node that connects to the guests. |

**Default** n/a

**Mode** User Exec/Privileged Exec

**Example 1** To display atmf area guest nodes on a controller, use the command,

```
GuestNode[1]#show atmf area guests
```

**Output** Figure 42-15: Example output from the **show atmf area guests** command

|                                            |                |                |       |              |
|--------------------------------------------|----------------|----------------|-------|--------------|
| main-building Area Guest Node Information: |                |                |       |              |
| Device                                     | MAC            |                |       | IP/IPv6      |
| Type                                       | Address        | Parent         | Port  | Address      |
| -----                                      |                |                |       |              |
| -                                          | 0008.5d10.7635 | x230           | 1.0.3 | 192.168.5.4  |
| AT-TQ4600                                  | eccd.6df2.da60 | wireless-node1 | 1.0.4 | 192.168.5.3  |
| -                                          | 0800.239e.f1fe | x230           | 1.0.4 | 192.168.4.8  |
| AT-TQ4600                                  | 001a.eb3b.dc80 | wireless-node2 | 1.0.7 | 192.168.4.12 |
| main-building guest node count 4           |                |                |       |              |
| GuestNode[1]#                              |                |                |       |              |

**Table 51:** Parameters in the output from **show atmf area guests** command

| Parameter   | Description                                                         |
|-------------|---------------------------------------------------------------------|
| Device Type | The device type as read from the guest node.                        |
| MAC Address | The MAC address of the guest-node                                   |
| Parent      | The device that directly connects to the guest-node                 |
| Port        | The port number on the parent node that connects to the guest node. |
| IP/IPv6     | The IP or IPv6 address of the guest node.                           |

**Related  
commands**

- [show atmf area](#)
- [show atmf area nodes](#)
- [show atmf backup guest](#)
- [show atmf area guests-detail](#)

# show atmf area guests-detail

**Overview** This command displays the local and remote guest information from an AMF controller.

**Syntax** show atmf area guests-detail [<area-name> [<node-name>]]

| Parameter   | Description                                                                                                  |
|-------------|--------------------------------------------------------------------------------------------------------------|
| <area-name> | The name assigned to the AMF area. An area is an AMF network that is under the control of an AMF Controller. |
| <node-name> | The name assigned to the network node.                                                                       |

**Default** n/a.

**Mode** Privileged Exec

**Example** To display detailed information for all guest nodes attached to “node1”, which is located within the area named “northern”, use the following command:

```
AMF_controller#show atmf area guests-detail northern node1
```

**Output** Figure 42-16: Example output from the **show atmf guest detail** command.

|                         |                  |
|-------------------------|------------------|
| #show atmf guest detail |                  |
| Node Name               | : Node1          |
| Port Name               | : port1.0.5      |
| Ifindex                 | : 5005           |
| Guest Description       | : tq4600         |
| Device Type             | : AT-TQ4600      |
| Configuration Mismatch  | : No             |
| Backup Supported        | : Yes            |
| MAC Address             | : eccd.6df2.da60 |
| IP Address              | : 192.168.4.50   |
| IPv6 Address            | : Not Set        |
| HTTP Port               | : 80             |
| Firmware Version        | :                |
| Node Name               | : poe            |
| Port Name               | : port1.0.6      |
| Ifindex                 | : 5006           |
| Guest Description       | : tq3600         |
| Device Type             | : AT-TQ2450      |
| Configuration Mismatch  | : No             |
| Backup Supported        | : Yes            |
| MAC Address             | : 001a.eb3b.cb80 |
| IP Address              | : 192.168.4.9    |
| IPv6 Address            | : Not Set        |
| HTTP Port               | : 80             |
| Firmware Version        | :                |

**Table 52:** Parameters shown in the output of the **show atmf guest detail** command

| Parameter         | Description                                                                                                                                                                               |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Node Name         | The name of the guest's parent node.                                                                                                                                                      |
| Port Name         | The port on the parent node that connects to the guest.                                                                                                                                   |
| IFindex           | An internal index number that maps to the port number on the parent node.                                                                                                                 |
| Guest Description | A brief description of the guest node as manually entered into the <a href="#">description (interface)</a> command for the guest node port on the parent node.                            |
| Device Type       | The device type as supplied by the guest node itself.                                                                                                                                     |
| Backup Supported  | Indicates whether AMF supports backup of this guest node.                                                                                                                                 |
| MAC Address       | The MAC address of the guest node.                                                                                                                                                        |
| IP Address        | The IP address of the guest node.                                                                                                                                                         |
| IPv6 Address      | The IPv6 address of the guest node.                                                                                                                                                       |
| HTTP Port         | The HTTP port enables you to specify a port when enabling http to allow a URL for the http user interface of a Guest Node. This is determined by the <a href="#">http-enable</a> command. |
| Firmware Version  | The firmware version that the guest node is currently running.                                                                                                                            |

**Related commands**   [show atmf area nodes-detail](#)  
[show atmf area guests](#)

# show atmf area nodes

**Overview** Use this command to display summarized information about an AMF controller's remote nodes.

Note that this command can only be run from a controller node.

**Syntax** `show atmf area nodes <area-name> [<node-name>]`

| Parameter   | Description                                             |
|-------------|---------------------------------------------------------|
| <area-name> | Displays information about nodes in the specified area. |
| <node-name> | Displays information about the specified node.          |

**Mode** Privileged Exec

**Usage notes** If you do not limit the output to a single area or node, this command lists all remote nodes that the controller is aware of. This can be a very large number of nodes.

**Example** To show summarized information for all the nodes in area 'Wellington', use the command:

```
controller-1# show atmf area nodes Wellington
```

The following figure shows partial example output from running this command.

**Table 53:** Output from the **show atmf area nodes Wellington** command

```
controller-1#show atmf area nodes Wellington
```

Wellington Area Node Information:

| Node        | Device        | ATMF   |    | Parent      | Node  |
|-------------|---------------|--------|----|-------------|-------|
| Name        | Type          | Master | SC | Domain      | Depth |
| -----       |               |        |    |             |       |
| well-gate   | x230-18GP     | N      | N  | well-master | 1     |
| well-master | AT-x930-28GPX | Y      | N  | none        | 0     |

Wellington node count 2

**Table 54:** Parameter definitions from the **show atmf area nodes** command

| Parameter   | Definition                                                                               |
|-------------|------------------------------------------------------------------------------------------|
| Node Name   | The name assigned to a particular node.                                                  |
| Device Type | The Product series name.                                                                 |
| ATMF Master | Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not). |



**Table 54:** Parameter definitions from the **show atmf area nodes** command

| Parameter     | Definition                                                                                            |
|---------------|-------------------------------------------------------------------------------------------------------|
| SC            | The device configuration, one of C - Chassis (SBx8100 series), S - Stackable (VCS) or N - Standalone. |
| Parent Domain | The node to which the current node has an active uplink.                                              |
| Node Depth    | The number of nodes in the path from this node to the master node.                                    |

**Related commands** [show atmf area](#)  
[show atmf area nodes-detail](#)

# show atmf area nodes-detail

**Overview** Use this command to display detailed information about an AMF controller's remote nodes.

Note that this command can only be run from a controller node.

**Syntax** `show atmf area nodes-detail <area-name> [<node-name>]`

| Parameter   | Description                                                      |
|-------------|------------------------------------------------------------------|
| <area-name> | Displays detailed information about nodes in the specified area. |
| <node-name> | Displays detailed information about the specified node.          |

**Mode** Privileged Exec

**Usage notes** If you do not limit the output to a single area or node, this command displays information about all remote nodes that the controller is aware of. This can be a very large number of nodes.

**Example** To show information for all the nodes in area 'Wellington', use the command:

```
controller-1# show atmf area nodes-detail Wellington
```

The following figure shows partial example output from running this command.

**Table 55:** Output from the **show atmf area nodes-detail Wellington** command

|                                                     |                        |
|-----------------------------------------------------|------------------------|
| controller-1#show atmf area nodes-detail Wellington |                        |
| Wellington Area Node Information:                   |                        |
| Node name                                           | well-gate              |
| Parent node name                                    | : well-master          |
| Domain id                                           | : well-gate's domain   |
| Board type                                          | : 368                  |
| Distance to core                                    | : 1                    |
| Flags                                               | : 50                   |
| Extra flags                                         | : 0x00000006           |
| MAC Address                                         | : 001a.eb56.9020       |
| Node name well-master                               |                        |
| Parent node name                                    | : none                 |
| Domain id                                           | : well-master's domain |
| Board type                                          | : 333                  |
| Distance to core                                    | : 0                    |
| Flags                                               | : 51                   |
| Extra flags                                         | : 0x0000000c           |
| MAC Address                                         | : eccd.6d3f.fef7       |
| ...                                                 |                        |

**Table 56:** Parameter definitions from the **show atmf area nodes-detail** command

| Parameter        | Definition                                                                            |
|------------------|---------------------------------------------------------------------------------------|
| Node name        | The name assigned to a particular node.                                               |
| Parent node name | The node to which the current node has an active uplink.                              |
| Domain id        | The name of the domain the node belongs to.                                           |
| Board type       | The Allied Telesis code number for the device.                                        |
| Distance to core | The number of nodes in the path from the current node to the master node in its area. |
| Flags            | Internal AMF information                                                              |
| Extra flags      | Internal AMF information                                                              |
| MAC Address      | The MAC address of the current node                                                   |

**Related commands**   [show atmf area](#)  
                              [show atmf area nodes](#)

# show atmf area summary

**Overview** Use this command to display a summary of IPv6 addresses used by AMF, for one or all of the areas controlled by an AMF controller.

**Syntax** `show atmf area summary [<area-name>]`

| Parameter   | Description                                       |
|-------------|---------------------------------------------------|
| <area-name> | Displays information for the specified area only. |

**Mode** Privileged Exec

**Example 1** To show a summary of IPv6 addresses used by AMF, for all of the areas controlled by controller-1, use the command:

```
controller-1# show atmf area summary
```

The following figure shows example output from running this command.

**Table 57:** Output from the **show atmf area summary** command

|                                     |                         |
|-------------------------------------|-------------------------|
| controller-1#show atmf area summary |                         |
| ATMF Area Summary Information:      |                         |
| Management Information              |                         |
| Local IPv6 Address                  | : fd00:4154:4d46:1::15  |
| Area Information                    |                         |
| Area Name                           | : NZ (Local)            |
| Area ID                             | : 1                     |
| Area Master IPv6 Address            | : -                     |
| Area Name                           | : Wellington            |
| Area ID                             | : 2                     |
| Area Master IPv6 Address            | : fd00:4154:4d46:2::149 |
| Area Name                           | : Canterbury            |
| Area ID                             | : 3                     |
| Area Master IPv6 Address            | : fd00:4154:4d46:3::f   |
| Area Name                           | : Auckland              |
| Area ID                             | : 100                   |
| Area Master IPv6 Address            | : fd00:4154:4d46:64::17 |
| Interface                           | : vlink2000             |

**Related commands**

- [show atmf area](#)
- [show atmf area nodes](#)
- [show atmf area nodes-detail](#)

# show atmf authorization

**Overview** Use this command on an AMF master to display the authorization status of other AMF members and masters on the network.

On an AMF controller this command will show the authorization status of remote area AMF masters.

**Syntax** `show atmf authorization {current|pending|provisional}`

| Parameter   | Description                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| current     | Show the status of all authorized nodes.                                                                                                                                                                    |
| pending     | Show the status of unauthorized nodes in the pending queue. These are nodes that enabled secure mode with <code>atmf secure-mode</code> but have not yet been authorized with <code>atmf authorize</code> . |
| provisional | Show the status of provisionally authorized nodes. These are nodes that have been provisioned with <code>atmf authorize provision</code> .                                                                  |

**Mode** Privileged Exec

**Example** To display all authorized AMF nodes on an AMF controller or AMF master, use the command:

```
awplus# show atmf authorization current
```

To display AMF nodes which are requesting authorization on an AMF controller or AMF master, use the command:

```
awplus# show atmf authorization pending
```

To display AMF nodes which have provisional authorization, use the command:

```
awplus# show atmf authorization provisional
```

**Output** Figure 42-17: Example output from **show atmf authorization current**

| NZ Authorized Nodes: |          |            |
|----------------------|----------|------------|
| Node Name            | Signer   | Expires    |
| -----                |          |            |
| master_1             | master_1 | 4 Mar 2017 |
| area_1_node_1        | master_1 | 4 Mar 2017 |
| area_1_node_2        | master_1 | 4 Mar 2017 |

Table 42-1: Parameters in the output from **show atmf authorization current**

| Parameter | Description                                                                                                                    |
|-----------|--------------------------------------------------------------------------------------------------------------------------------|
| Node Name | AMF node name of the authorized node.                                                                                          |
| Signer    | Name of the AMF master that authorized the node.                                                                               |
| Expires   | Expiry date of the authorization. Authorization expiry time is set using <a href="#">atmf secure-mode certificate expiry</a> . |

**Output** Figure 42-18: Example output from **show atmf authorization pending**

|                         |            |             |           |
|-------------------------|------------|-------------|-----------|
| Pending Authorizations: |            |             |           |
| NZ Requests:            |            |             |           |
| Node Name               | Product    | Parent Node | Interface |
| -----                   | -----      | -----       | -----     |
| area_1_node_3           | x230-18GP  | master_1    | port1.2.9 |
| area_1_node_4           | x510-52GTX | master_1    | sa1       |

Table 42-2: Parameters in the output from **show atmf authorization pending**

| Parameter   | Description                                          |
|-------------|------------------------------------------------------|
| Node Name   | Name of the node that is requesting authorization.   |
| Product     | Product name.                                        |
| Parent Node | Authorization authority of the requesting node.      |
| Interface   | Interface that the authorization request came in on. |

**Output** Figure 42-19: Example output from **show atmf authorization provisional**

|                                 |                     |           |         |
|---------------------------------|---------------------|-----------|---------|
| ATMF Provisional Authorization: |                     |           |         |
| Area - Node Name                | Start               | Timeout   |         |
| or MAC Address                  | Time                | Interface | Minutes |
| -----                           | -----               | -----     | -----   |
| 3333.4444.5555                  | 5 Sep 2016 02:35:54 |           | 3       |
| 1111.2222.3333                  | 5 Sep 2016 02:35:24 |           | 60      |
| NZ - blue                       | 5 Sep 2016 02:35:06 | port1.0.3 | 60      |

Table 42-3: Parameters in the output from **show atmf authorization provisional**

| Parameter                          | Description                                                                  |
|------------------------------------|------------------------------------------------------------------------------|
| Area - Node Name<br>or MAC Address | MAC address or node name of the node that has been provisionally authorized. |
| Interface                          | Interface that the node has been provisioned on.                             |
| Start Time                         | Time the node was provisioned.                                               |
| Timeout Minutes                    | Length of time from Start Time until the provisional authorization expires.  |

**Related  
commands**

[atmf authorize](#)  
[atmf authorize provision](#)  
[atmf secure-mode](#)  
[clear atmf secure-mode certificates](#)  
[show atmf](#)  
[show atmf secure-mode](#)  
[show atmf secure-mode certificates](#)

**Command  
changes**

Version 5.4.7-0.3: command added

# show atmf backup

**Overview** This command displays information about AMF backup status for all the nodes in an AMF network. It can only be run on AMF master and controller nodes.

**Syntax**

```
show atmf backup
show atmf backup logs
show atmf backup server-status
show atmf backup synchronize [logs]
```

| Parameter     | Description                                                                           |
|---------------|---------------------------------------------------------------------------------------|
| logs          | Displays detailed log information.                                                    |
| server-status | Displays connectivity diagnostics information for each configured remote file server. |
| synchronize   | Display the file server synchronization status                                        |
| logs          | For each remote file server, display the logs for the last synchronization            |

**Mode** Privileged Exec

**Example 1** To display the AMF backup information, use the command:

```
node_1# show atmf backup
```

To display log messages to do with backups, use the command:

```
node_1# show atmf backup logs
```

Table 42-4: Output from **show atmf backup**

|                                                     |             |          |         |          |             |
|-----------------------------------------------------|-------------|----------|---------|----------|-------------|
| Node_1# show atmf backup                            |             |          |         |          |             |
| ScheduledBackup .....Enabled                        |             |          |         |          |             |
| Schedule.....1 per day starting at 03:00            |             |          |         |          |             |
| Next Backup Time....04 May 2019 03:00               |             |          |         |          |             |
| Backup Bandwidth ....Unlimited                      |             |          |         |          |             |
| Backup Media.....SD (Total 1974.0 MB, Free197.6MB)  |             |          |         |          |             |
| Current Action.....Starting manual backup           |             |          |         |          |             |
| Started.....04 May 2019 10:08                       |             |          |         |          |             |
| CurrentNode.....atmf_testbox1                       |             |          |         |          |             |
| Backup Redundancy ...Enabled                        |             |          |         |          |             |
| Local media .....SD (Total 3788.0MB, Free 3679.5MB) |             |          |         |          |             |
| State .....Active                                   |             |          |         |          |             |
| Node Name                                           | Date        | Time     | In ATMF | On Media | Status      |
| -----                                               |             |          |         |          |             |
| atmf_testbox1                                       | 04 May 2019 | 09:58:59 | Yes     | Yes      | In Progress |
| atmf_testbox2                                       | 04 May 2019 | 10:01:23 | Yes     | Yes      | Good        |



Table 42-5: Output from **show atmf backup logs**

```
Node_1#show atmf backup logs

Backup Redundancy Enabled
Local media SD (Total 3788.0MB, Free 1792.8MB)
State Inactive (Remote file server is not available)

Log File Location: card:/atmf/ATMF/logs/rsync_<node name>.log

Node
Name Log Details

atmf_testbox
2019/05/04 18:16:51 [9045] receiving file list
2019/05/04 18:16:51 [9047] .d..t.... flash/
2019/05/04 18:16:52 [9047] >f+++++++ flash/a.rel
```

**Example 2** To display the AMF backup synchronization status, use the command:

```
node_1# show atmf backup synchronize
```

To display log messages to do with synchronization of backups, use the command:

```
node_1# show atmf backup synchronize logs
```

Table 42-6: Output from **show atmf backup synchronize**

```
Node_1#show atmf backup synchronize

ATMF backup synchronization:

* = Active file server

 Id Date Time Status

 1 04 May 2016 22:25:57 Synchronized
* 2 - - Active
```

Table 42-7: Output from **show atmf backup synchronize logs**

```
Node_1#show atmf backup synchronize logs

Id Log Details

1 2019/05/04 22:25:54 [8039] receiving file list
 2019/05/04 22:25:54 [8039] >f..t.... backup_Box1.info
 2019/05/04 22:25:54 [8039] sent 46 bytes received 39 bytes total size 40
```

**Example 3** To display the AMF backup information with the optional parameter **server-status**, use the command:

```
Node_1# show atmf backup server-status
```

```
Node1#sh atmf backup server-status

Id Last Check State

1 186 s File server ready
2 1 s SSH no route to host
```

**Table 43:** Parameter definitions from the **show atmf backup** command

| Parameter         | Definition                                                                                                                                                                                                                                  |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Scheduled Backup  | Indicates whether AMF backup scheduling is enabled or disabled.                                                                                                                                                                             |
| Schedule          | Displays the configured backup schedule.                                                                                                                                                                                                    |
| Next Backup Time  | Displays the date and time of the next scheduled.                                                                                                                                                                                           |
| Backup Media      | The current backup medium in use.<br>This will be SD or NONE. SD card only (and not USB) is supported for AMF backup. Utilized and available memory (MB) will be indicated if backup media memory is present.                               |
| Current Action    | The task that the AMF backup mechanism is currently performing. This will be a combination of either (Idle, Starting, Doing, Stopping), or (manual, scheduled).                                                                             |
| Started           | The date and time that the currently executing task was initiated in the format DD MMM YYYY HH:MM                                                                                                                                           |
| Current Node      | The name of the node that is currently being backed up.                                                                                                                                                                                     |
| Backup Redundancy | Whether backup redundancy is enabled or disabled.                                                                                                                                                                                           |
| Local media       | The local media to be used for backup redundancy; SD, USB, INTERNAL, or NONE, and total and free memory available on the media.                                                                                                             |
| State             | Whether SD or USB media is installed and available for backup redundancy. May be Active (if backup redundancy is functional—requires both the local redundant backup media and a remote server to be configured and available) or Inactive. |
| Node Name         | The name of the node that is storing backup data - on its backup media.                                                                                                                                                                     |
| Date              | The data of the last backup in the format DD MMM YYYY.                                                                                                                                                                                      |
| Time              | The time of the last backup in the format HH:MM:SS.                                                                                                                                                                                         |
| In ATMF           | Whether the node shown is active in the AMF network, (Yes or No).                                                                                                                                                                           |
| On Media          | Whether the node shown has a backup on the backup media (Yes or No).                                                                                                                                                                        |

**Table 43:** Parameter definitions from the **show atmf backup** command (cont.)

| Parameter         | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Status            | The output can contain one of four values: <ul style="list-style-type: none"><li>• “-” meaning that the status file cannot be found or cannot be read.</li><li>• “Errors” meaning that there are issues - note that the backup may still be deemed successful depending on the errors.</li><li>• “Stopped” meaning that the backup attempt was manually aborted.</li><li>• “Good” meaning that the backup was completed successfully.</li><li>• “In Progress” meaning that the backup is currently running on that node.</li></ul> |
| Log File Location | All backup attempts will generate a result log file in the identified directory based on the node name. In the above example this would be:<br>card:/amf/office/logs/rsync_amf_testbox1.log.                                                                                                                                                                                                                                                                                                                                       |
| Log Details       | The contents of the backup log file.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| server-status     | Displays connectivity diagnostics information for each configured remove file server.                                                                                                                                                                                                                                                                                                                                                                                                                                              |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Related commands**    [show atmf](#)  
                          [atmf network-name](#)

# show atmf backup area

**Overview** Use this command to display backup status information for the master nodes in one or more areas.

Note that this command is only available on AMF controllers.

**Syntax** `show atmf backup area [<area-name> [<node-name>]] [logs]`

| Parameter   | Description                                             |
|-------------|---------------------------------------------------------|
| logs        | Displays the logs for the last backup of each node.     |
| <area-name> | Displays information about nodes in the specified area. |
| <node-name> | Displays information about the specified node.          |

**Mode** Privileged Exec

**Example** To show information about backups for an area, use the command:

```
controller-1# show atmf backup area
```

**Table 44:** Output from the **show atmf backup area** command

```

controller-1#show atmf backup area

Scheduled Backup Enabled
 Schedule 12 per day starting at 14:30
 Next Backup Time 15 Oct 2016 04:30
Backup Bandwidth Unlimited
Backup Media FILE SERVER 1 (Total 128886.5MB, Free 26234.2MB)
Server Config
 * 1 Configured (Mounted, Active)
 Host 10.37.74.1
 Username root
 Path /tftpboot/backups_from_controller-1
 Port -
 2 Configured (Unmounted)
 Host 10.37.142.1
 Username root
 Path -
 Port -
Current Action Idle
 Started -
 Current Node -

Backup Redundancy Enabled
 Local media USB (Total 7604.0MB, Free 7544.0MB)
 State Active

```

| Area Name  | Node Name | Id | Date        | Time     | Status |
|------------|-----------|----|-------------|----------|--------|
| Wellington | camry     | 1  | 14 Oct 2016 | 02:30:22 | Good   |
| Canterbury | corona    | 1  | 14 Oct 2016 | 02:30:23 | Good   |
| Canterbury | Avensis   | 1  | 14 Oct 2016 | 02:30:22 | Good   |
| Auckland   | RAV4      | 1  | 14 Oct 2016 | 02:30:23 | Good   |
| Southland  | MR2       | 1  | 14 Oct 2016 | 02:30:24 | Good   |

**Related commands**

- [atmf backup area-masters enable](#)
- [show atmf area](#)
- [show atmf area nodes-detail](#)
- [switchport atmf-arealink](#)

# show atmf backup guest

**Overview** This command displays backup status information of guest nodes in an AMF network. This command can only be run on a device configured as an AMF Master and has an AMF guest license.

**Syntax** `show atmf backup guest [<node-name> [<guest-port>]] [logs]`

| Parameter    | Description                        |
|--------------|------------------------------------|
| <node-name>  | The name of parent guest node      |
| <guest-port> | The port number on the parent node |

**Mode** User Exec/Privileged Exec

**Example** On the switch named x930-master, to display information about the AMF backup guest status, use the command:

```
x930-master# show atmf backup guest
```

**Output** Figure 42-20: Example output from **show atmf backup guest**

```
x930-master#sh atmf backup guest
Guest Backup Enabled
Scheduled Backup Disabled
 Schedule 1 per day starting at 03:00
 Next Backup Time 20 Jan 2016 03:00
Backup Bandwidth Unlimited
Backup Media FILE SERVER 2 (Total 655027.5MB,
 Free 140191.5MB)
Server Config
 1 Configured (Mounted)
 Host 11.0.24.1
 Username bob
 Path guest-project
 Port -
* 2 Configured (Mounted, Active)
 Host 11.0.24.1
 Username bob
 Path guest-project-second
 Port.....-
Current Action Idle
Started -
Current Node -
Backup Redundancy ...Enabled
Local media USB (Total 7376.0MB, Free 7264.1MB)
State Active
```

| Parent Node Name | Port Name | Id  | Date        | Time     | Status |
|------------------|-----------|-----|-------------|----------|--------|
| <hr/>            |           |     |             |          |        |
| x230             | port1.0.4 | 2   | 19 Jan 2016 | 22:21:46 | Good   |
|                  |           | 1   | 19 Jan 2016 | 22:21:46 | Good   |
|                  |           | USB | 19 Jan 2016 | 22:21:46 | Good   |

Table 42-1: Parameters in the output from **show atmf backup guest**

| Parameter        | Description                                                                                                                                                                |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Guest Backup     | The status of the guest node backup process                                                                                                                                |
| Scheduled Backup | The timing configured for guest backups.                                                                                                                                   |
| Schedule         | Displays the configured backup schedule.                                                                                                                                   |
| Next Backup Time | The time the next backup process will be initiated.                                                                                                                        |
| Backup Bandwidth | The bandwidth limit applied to the backup data flow measured in kilo Bytes /second. Note that unlimited means there is no limit set specifically for the backup data flow. |
| Backup Media     | Detail of the memory media used to store the backup files and the current memory capacity available.                                                                       |

**Related commands**

- [show atmf backup area](#)
- [show atmf backup](#)
- [show atmf links guest](#)
- [show atmf nodes](#)
- [show atmf backup guest](#)
- [atmf backup guests delete](#)
- [atmf backup guests enable](#)

# show atmf container

**Overview** Use this command to display information about the AMF containers created on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

**Syntax** `show atmf container [detail] [<container-name>]`

| Parameter        | Description                                                        |
|------------------|--------------------------------------------------------------------|
| detail           | Show detailed information.                                         |
| <container-name> | The name of the AMF container you wish to display information for. |

**Mode** Privileged Exec

**Output** Figure 42-21: Example output from **show atmf container**

```
awplus#show atmf container
```

ATMF Container Information:

| Container | Area | Bridge | State   | Memory  | CPU% |
|-----------|------|--------|---------|---------|------|
| vac-wlg-1 | wlg  | br1    | running | 70.3 MB | 1.2  |
| vac-akl-1 | akl  | br2    | stopped | 0 bytes | 0.0  |
| vac-nsn-1 | nsn  | br3    | running | 53.2 MB | 0.7  |

Current ATMF Container count: 3

Figure 42-22: Example output from **show atmf container vac-wlg-1**

```
awplus#show atmf container vac-wlg-1
```

ATMF Container Information:

| Container | Area | Bridge | State   | Memory  | CPU% |
|-----------|------|--------|---------|---------|------|
| vac-wlg-1 | wlg  | br1    | running | 70.3 MB | 1.2  |

Current ATMF Container count: 1



Table 42-2: Parameters in the output from **show atmf container**

| Parameter | Description                                                                                                      |
|-----------|------------------------------------------------------------------------------------------------------------------|
| Container | Name of the AMF container.                                                                                       |
| Area      | Name of the area the container is in.                                                                            |
| Bridge    | Name of the bridge connecting the container to the physical network.                                             |
| State     | Container state, <code>running</code> or <code>stopped</code> . This is set with the <code>state</code> command. |
| Memory    | The amount of memory the container is using on the VAA host.                                                     |
| CPU%      | The percentage of CPU time the container is using on the VAA, at the time the show command is run.               |

Figure 42-23: Example output from **show atmf container detail vac-wlg-1**

```
awplus#show atmf container detail vac-wlg-1

ATMF Container Information:

Name: vac-wlg-1
State: RUNNING
PID: 980
IP: 172.31.0.1
IP: 192.168.0.2
IP: fd00:4154:4d46:3c::1
CPU use: 3.95 seconds
Memory use: 67.07 MiB
Memory use: 0 bytes
Link: vethP31UFA
TX bytes: 166.01 KiB
RX bytes: 141.44 KiB
Total bytes: 307.45 KiB
Link: vethYCT7BB
TX bytes: 674.27 KiB
RX bytes: 698.27 KiB
Total bytes: 1.34 MiB
```

Table 42-3: Parameters in the output from **show atmf container detail**

| Parameter | Description                                                                                                      |
|-----------|------------------------------------------------------------------------------------------------------------------|
| Name      | Name of the AMF container.                                                                                       |
| State     | Container state, <code>RUNNING</code> or <code>STOPPED</code> . This is set with the <code>state</code> command. |

Table 42-3: Parameters in the output from **show atmf container detail** (cont.)

| Parameter   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| PID         | Internal container id.                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| IP          | This lists the IP addresses used by the container. These include the eth1 IP address and the AMF management IP address.                                                                                                                                                                                                                                                                                                                                                |
| CPU use     | The CPU usage of the container since it was enabled.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Memory use  | Container memory usage.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Link        | Each container has two links:<br><ol style="list-style-type: none"><li>1 An AMF area-link, this connects the container to the AMF controller and uses virtual interface eth0 on the AMF container.</li><li>2 A bridged L2 network link, this connects the container to the outside world and uses the virtual interface eth1 on the AMF container.</li></ol> See the <a href="#">AMF Feature Overview and Configuration_Guide</a> for more information on these links. |
| TX/RX bytes | Bytes sent and received on a link.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Total bytes | Total bytes transferred on a link.                                                                                                                                                                                                                                                                                                                                                                                                                                     |

**Related  
commands**

[area-link](#)  
[atmf area](#)  
[atmf area password](#)  
[atmf container](#)  
[atmf container login](#)  
[bridge-group \(amf-container\)](#)  
[description \(amf-container\)](#)  
[state](#)

**Command  
changes**

Version 5.4.7-0.1: command added

# show atmf detail

**Overview** This command displays details about an AMF node. It can only be run on AMF master and controller nodes.

**Syntax** `show atmf detail`

| Parameter | Description                       |
|-----------|-----------------------------------|
| detail    | Displays output in greater depth. |

**Mode** Privileged Exec

**Example 1** To display the AMF node1 information in detail, use the command:

```
controller-1# show atmf detail
```

A typical output screen from this command is shown below:

```
atmf-1#show atmf detail
ATMF Detail Information:

Network Name : Test_network
Network Mtu : 1300
Node Name : controller-1
Node Address : controller-1.atmf
Node ID : 342
Node Depth : 0
Domain State : BackupDomainController
Recovery State : None
Recovery Over ETH Ports : Disabled
Log Verbose Setting : Verbose
Topology GUI : Disabled

Management VLAN
VLAN ID : 4000
Management Subnet : 172.31.0.0
Management IP Address : 172.31.1.86
Management Mask : 255.255.128.0
Management IPv6 Address : fd00:4154:4d46:1::156
Management IPv6 Prefix Length : 64

Domain VLAN
VLAN ID : 4091
Domain Subnet : 172.31.128.0
Domain IP Address : 172.31.129.86
Domain Mask : 255.255.128.0
```

**Table 43:** Parameter definitions from the **show atmf detail** command

| Parameter               | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network MTU             | The network MTU for the ATMF network.                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Network Name            | The AMF network that a particular node belongs to.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Node Name               | The name assigned to a particular node.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Node Address            | An address used to access a remotely located node. This is simply the Node Name plus the dotted suffix atmf (.atmf).                                                                                                                                                                                                                                                                                                                                                 |
| Node ID                 | A unique identifier assigned to a node on an AMF network.                                                                                                                                                                                                                                                                                                                                                                                                            |
| Node Depth              | The number of nodes in the path from this node to the level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.                                                                                                                                                                                                                                                       |
| Domain State            | The state of a node in a Domain in an AMF network as Controller/Backup.                                                                                                                                                                                                                                                                                                                                                                                              |
| Recovery State          | The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.                                                                                                                                                                                                                                                                                                                                               |
| Recovery Over ETH Ports | Allow AMF recovery over the Eth port on an AR-series device.                                                                                                                                                                                                                                                                                                                                                                                                         |
| Log Verbose Setting     | The state of the <a href="#">atmf log-verbose</a> command.                                                                                                                                                                                                                                                                                                                                                                                                           |
| Topology GUI            | This feature allows your AMF network to interact with Vista Manager EX and must be enabled on your AMF master.                                                                                                                                                                                                                                                                                                                                                       |
| Management VLAN         | The VLAN created for traffic between nodes of different domain (up/down links). <ul style="list-style-type: none"> <li>• VLAN ID - in this example VLAN 4092 is configured as the Management VLAN.</li> <li>• Management Subnet - the network prefix for the subnet.</li> <li>• Management IP Address - the IP address allocated for this traffic.</li> <li>• Management Mask - the subnet mask used to create a subnet for this traffic (255.255.128.0).</li> </ul> |
| Domain VLAN             | The VLAN assigned for traffic between nodes of the same domain (crosslink). <ul style="list-style-type: none"> <li>• VLAN ID - in this example VLAN 4091 is configured as the domain VLAN.</li> <li>• Domain Subnet - the subnet address used for this traffic.</li> <li>• Domain IP Address - the IP address allocated for this traffic.</li> <li>• Domain Mask - the subnet mask used to create a subnet for this traffic (255.255.128.0).</li> </ul>              |
| Node Depth              | The number of nodes in the path from this node to the core domain.                                                                                                                                                                                                                                                                                                                                                                                                   |

# show atmf group

**Overview** This command can be used to display the group membership within to a particular AMF node. It can also be used with the working-set command to display group membership within a working set.

Each node in the AMF is automatically added to the group that is appropriate to its hardware architecture, e.g. x510, x230. Nodes that are configured as masters are automatically assigned to the master group.

You can create arbitrary groups of AMF members based on your own selection criteria. You can then assign commands collectively to any of these groups.

**Syntax** `show atmf group [user-defined|automatic]`

| Parameter    | Description                             |
|--------------|-----------------------------------------|
| user-defined | User-defined-group information display. |
| automatic    | Automatic group information display.    |

**Default** All groups are displayed

**Mode** Privileged Exec

**Example 1** To display group membership of node2, use the following command:

```
node2# show atmf group
```

A typical output screen from this command is shown below:

```
ATMF group information

master, x510

node2#
```

This screen shows that node2 contains the groups **master** and **x510**. Note that although the node also contains the implicit groups, these do not appear in the show output.

**Example 2** The following commands (entered on *node2*) will display all the automatic groups within the working set containing *node1* and all nodes that have been pre-defined to contain the *sysadmin* group:

First define the working-set:

```
node1# #atmf working-set node1 group sysadmin
```

A typical output screen from this command is shown below:

```

ATMF group information

master, poe, x8100

=====
node1, node2, node3, node4, node5, node6:
=====

ATMF group information

sysadmin, x8100

AMF_NETWORK[6]#

```

This confirms that the six nodes (*node1* to *node6*) are now members of the working-set and that these nodes reside within the *AMF-NETWORK*.

Note that to run this command, you must have previously entered the command [atmf working-set](#) on page 1972. This can be seen from the network level prompt, which in this case is *AMF\_NETWORK[6]#*.

**Table 44:** Sample output from the **show atmf group** command for a working set.

```

AMF_NETWORK[6]#show atmf group
=====
node3, node4, node5, node6:
=====

ATMF group information

edge_switches, x510

```

**Table 45:** Parameter definitions from the **show atmf group** command for a working set

| Parameter              | Definition                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ATMF group information | <p>Displays a list of nodes and the groups that they belong to, for example:</p> <ul style="list-style-type: none"> <li>• master - Shows a common group name for Nodes configured as AMF masters.</li> <li>• Hardware Arch - Shows a group for all Nodes sharing a common Hardware architecture, e.g. x8100, x230, for example.</li> <li>• User-defined - Arbitrary groups created by the user for AMF nodes.</li> </ul> |

# show atmf group members

**Overview** This command will display all group memberships within an AMF working-set. Each node in the AMF working set is automatically added to automatic groups which are defined by hardware architecture, e.g. x510, x230. Nodes that are configured as masters are automatically assigned to the master group. Users can define arbitrary groupings of AMF members based on their own criteria, which can be used to select groups of nodes.

**Syntax** `show atmf group members [user-defined|automatic]`

| Parameter    | Description                            |
|--------------|----------------------------------------|
| user-defined | User defined group membership display. |
| automatic    | Automatic group membership display.    |

**Mode** Privileged Exec

**Example** To display group membership of all nodes in a working-set, use the command:

```
ATMF_NETWORK[9]# show atmf group members
```

**Table 46:** Sample output from the **show atmf group members** command

|                       |               |                            |
|-----------------------|---------------|----------------------------|
| ATMF Group membership |               |                            |
| Automatic Groups      | Total Members | Members                    |
| -----                 |               |                            |
| master                | 1             | Building_1                 |
| poe                   | 1             | HW_Team1                   |
| x510                  | 3             | SW_Team1 SW_Team2 SW_Team3 |
| x930                  | 1             | HW_Team1                   |
| x8100                 | 2             | Building_1 Building_2      |
| ATMF Group membership |               |                            |
| User-defined Groups   | Total Members | Members                    |
| -----                 |               |                            |
| marketing             | 1             | Bld1_Floor_1               |
| software              | 3             | SW_Team1 SW_Team2 SW_Team3 |

**Table 47:** Parameter definitions from the **show atmf group members** command

| Parameter           | Definition                                                                                                                                                       |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Automatic Groups    | Lists the Automatic Groups and their nodal composition. The sample output shows AMF nodes based on the same Hardware type or belonging to the same Master group. |
| User-defined Groups | Shows the grouping of AMF nodes in user defined groups.                                                                                                          |
| Total Members       | Shows the total number of members in each group.                                                                                                                 |
| Members             | Shows the list of AMF nodes in each group.                                                                                                                       |

**Related commands**

- [show atmf group](#)
- [show atmf](#)
- [atmf group \(membership\)](#)



# show atmf guests

**Overview** This command is available on any AMF master or controller in the network. It displays a summary of the AMF guest nodes that exist in the AMF network, including device type, parent node, and IP address.

**Syntax** `show atmf guests`

**Mode** User Exec/Privileged Exec

**Usage notes** Use this command to display all guest nodes in a network. If you want to see only the guests attached to a single node, use the [show atmf links guest](#) command, which shows information about the guest nodes and also about their link to their parent node.

**Example** To display the AMF guest output, use the command:

```
awplus# show atmf guests
```

**Output** Figure 42-24: Example output from the **show atmf guests** command

```
master#show atmf guests

Guest Information:

Device Device Parent Guest IP/IPv6
Name Type Node Port Address

node1-2.0.1 x600-24Ts node1 2.0.1 192.168.2.10
wireless-zone1 AT-TQ4600 node2 1.0.1 192.168.1.10
wireless-zone2 AT-TQ4600 node2 1.0.2 192.168.1.12

Current ATMF guest node count 3
```

**Table 48:** Parameters shown in the output of the **show atmf guests** command

| Parameter   | Description                                                                                                                                                                                                                                          |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Name | The name that is discovered from the device, or failing that, a name that is auto-assigned by AMF. The auto-assigned name consists of:<br><parent node name>-<attached port number><br>You can change this by configuring a description on the port. |
| Device Type | The product name of the guest node, which is discovered from the device. If no device type can be discovered, this shows the name of the AMF guest-class that has been assigned to the guest node by the <a href="#">atmf guest-class</a> command.   |

**Table 48:** Parameters shown in the output of the **show atmf guests** command

| Parameter       | Description                                                                                        |
|-----------------|----------------------------------------------------------------------------------------------------|
| Parent Node     | The name of the AMF node that directly connects to the guest node.                                 |
| Guest Port      | The port on the parent node that directly connects to the guest node.                              |
| IP/IPv6 Address | The address discovered from the node, or statically configured on the parent node's attached port. |

**Related  
commands**

[atmf guest-class](#)  
[switchport atmf-guestlink](#)  
[show atmf backup guest](#)  
[show atmf links guest](#)

# show atmf guests detail

**Overview** This command is available on any AMF master in the network. It displays details about the AMF guest nodes that exist in the AMF network, such as device type, IP address, MAC address etc.

**Syntax** `show atmf guests detail [<node-name>] [<guest-port>]`

| Parameter                       | Description                          |
|---------------------------------|--------------------------------------|
| <code>&lt;node-name&gt;</code>  | The name of the guest node's parent. |
| <code>&lt;guest-port&gt;</code> | The port name on the parent node.    |

**Mode** User Exec/Privileged Exec

**Usage notes** If you want to see only the guests attached to a single node, you can use either:

- this command and specify the node name, or
- [show atmf links guest detail](#), which shows information about the guest nodes and also about their link to their parent node.

Note that the parameters that are displayed depend on the guest node's model.

**Example** To display the AMF guest output, use the command:

```
awplus# show atmf guests detail
```

**Output** Figure 42-25: Example output from **show atmf guests detail**

```
master#show atmf guests detail

ATMF Guest Node Information:

Node Name : master
Port Name : port1.0.9
Ifindex : 5009
Guest Description : red-1.0.9
Device Type : x600-24Ts
Backup Supported : No
MAC Address : 0000.cd38.0c4d
IP Address : 192.168.1.5
IPv6 Address : Not Set
HTTP Port : 0
Firmware Version : 5.4.2-0.1
```

|                   |                  |
|-------------------|------------------|
| Node Name         | : node1          |
| Port Name         | : port1.0.13     |
| Ifindex           | : 5013           |
| Guest Description | : node1-1.0.13   |
| Device Type       | : AT-TQ4600      |
| Backup Supported  | : Yes            |
| MAC Address       | : eccd.6df2.daa0 |
| IP Address        | : 192.168.5.6    |
| IPv6 Address      | : Not Set        |
| HTTP Port         | : 80             |
| Firmware Version  | : 3.1.0 B01      |

**Table 49:** Parameters in the output from **show atmf guests detail**.

| Parameter         | Description                                                                                                                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Node Name         | The name of the parent node, which is the AMF node that directly connects to the guest node.                                                                                                                                                       |
| Port Name         | The port on the parent node that connects to the guest.                                                                                                                                                                                            |
| IfIndex           | An internal index number that maps to the port number on the parent node.                                                                                                                                                                          |
| Guest Description | A description that is discovered from the device, or failing that, auto-assigned by AMF. The auto-assigned name consists of:<br><parent node name>-<attached port number>.<br>You can change this by configuring a description on the port.        |
| Device Type       | The product name of the guest node, which is discovered from the device. If no device type can be discovered, this shows the name of the AMF guest-class that has been assigned to the guest node by the <a href="#">atmf guest-class</a> command. |
| Username          | The user name configured on the guest node.                                                                                                                                                                                                        |
| Backup Supported  | Whether the guest node supports AMF backup functionality.                                                                                                                                                                                          |
| MAC Address       | The MAC address of the guest node.                                                                                                                                                                                                                 |
| IP Address        | The IP address of the guest node.                                                                                                                                                                                                                  |
| IPv6 Address      | The IPv6 address of the guest node.                                                                                                                                                                                                                |
| Firmware Version  | The version of the firmware operating on the guest node.                                                                                                                                                                                           |
| HTTP port         | The HTTP port as specified with the <a href="#">http-enable</a> command when defining a guest class. You can set this if the guest node provides an HTTP user interface on a non-standard port (any port other than port 80).                      |

**Related  
commands**   [atmf guest-class](#)  
[switchport atmf-guestlink](#)  
[show atmf backup guest](#)

# show atmf links

**Overview** This command displays information about AMF links on a switch. The display output contains link status state information.

**Syntax** `show atmf links [brief]`

| Parameter | Description                                                   |
|-----------|---------------------------------------------------------------|
| brief     | A brief summary of AMF links, their configuration and status. |

**Mode** User Exec and Privileged Exec

**Usage notes** The **show atmf links** and **show atmf links brief** commands both produce a table of summarized link information. For a more detailed view use the [show atmf links detail](#) command.

This command does not show links that are configured on provisioned ports.

**Example** To display a brief summary of the AMF links, use the following command:

```
node-1# show atmf links brief
```

Figure 42-26: Example output from **show atmf links brief**

| Example-core# show atmf links |           |             |            |               |                  |            |
|-------------------------------|-----------|-------------|------------|---------------|------------------|------------|
| ATMF Link Brief Information:  |           |             |            |               |                  |            |
| Local Port                    | Link Type | Link Status | ATMF State | Adjacent Node | Adjacent Ifindex | Link State |
| 1.0.10                        | Crosslink | Down        | Init       | *crosslink1   | -                | Blocking   |
| 1.0.14                        | Crosslink | Down        | Init       | *crosslink2   | -                | Blocking   |
| 1.0.1                         | Downlink  | Down        | Init       | -             | -                | Blocking   |
| 1.0.2                         | Downlink  | Up          | Full       | Node2         | 5001             | Forwarding |
| 1.0.8                         | Downlink  | Up          | Full       | downlink1     | 5001             | Forwarding |
| * = Provisioned.              |           |             |            |               |                  |            |

Table 42-1: Parameter in the output from **show atmf links brief**

| Parameter   | Definition                                                                                     |
|-------------|------------------------------------------------------------------------------------------------|
| Local Port  | Shows the local port on the selected node.                                                     |
| Link Type   | Shows link type as Uplink or Downlink (parent and child) or Cross-link (nodes in same domain). |
| Link Status | Shows the link status of the local port on the node as either Up or Down.                      |

Table 42-1: Parameter in the output from **show atmf links brief** (cont.)

| Parameter         | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ATMF State        | Shows AMF state of the local port: <ul style="list-style-type: none"><li>• Init - Link is down.</li><li>• Hold - Link transitioned to up state, but waiting for hold period to ensure link is stable.</li><li>• Incompatible - Neighbor rejected the link because of inconsistency in AMF configurations.</li><li>• OneWay - Link is up and has waited the hold down period and now attempting to link to another unit in another domain.</li><li>• OneWaySim - Device is running in secure mode and link is up but waiting for authorization from an AMF master.</li><li>• Full - Link hello packets are sent and received from its neighbor with its own node id.</li><li>• Shutdown - Link has been shut down by user configuration.</li></ul> |
| Adjacent Node     | Shows the Adjacent AMF Node to the one being configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Adjacent IF Index | Shows the IF index for the Adjacent AMF Node connected to the node being configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Link State        | Shows the state of the AMF link. Valid states are either Forwarding or Blocking.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare\\_Plus” Feature Overview and Configuration Guide](#).

**Related commands**

- [no debug all](#)
- [clear atmf links statistics](#)
- [show atmf](#)
- [show atmf links detail](#)
- [show atmf links guest](#)
- [show atmf links guest detail](#)
- [show atmf links statistics](#)
- [show atmf nodes](#)

# show atmf links detail

**Overview** This command displays detailed information on all the links configured in the AMF network. It can only be run on AMF master and controller nodes.

**Syntax** `show atmf links detail`

| Parameter | Description                     |
|-----------|---------------------------------|
| detail    | Detailed AMF links information. |

**Mode** User Exec

**Usage notes** For summarized link information see the [show atmf links](#) command.  
This command does not show links that are configured on provisioned ports.

**Example** To display the AMF link details use this command:

```
device1# show atmf links detail
```

The output from this command will display all the internal data held for AMF links. The following example gives details of the links that are summarized in the example in [show atmf links](#).

**Table 43:** Sample output from the **show atmf links detail** command

|                                 |                     |
|---------------------------------|---------------------|
| device1# show atmf links detail |                     |
| -----                           |                     |
| Crosslink Ports Information     |                     |
| -----                           |                     |
| Port                            | : sa1               |
| Ifindex                         | : 4501              |
| Port Status                     | : Down              |
| Port State                      | : Init              |
| Last event                      | :                   |
| Port BPDU Receive Count         | : 0                 |
| Port                            | : po10              |
| Ifindex                         | : 4610              |
| Port Status                     | : Up                |
| Port State                      | : Full              |
| Last event                      | : AdjNodeLSEPresent |
| Port BPDU Receive Count         | : 140               |
| Adjacent Node Name              | : Building-B        |
| Adjacent Ifindex                | : 4610              |
| Adjacent MAC                    | : eccd.6ddl.64d0    |
| Port Last Message Response      | : 0                 |



**Table 43:** Sample output from the **show atmf links detail** command (cont.)

|                                |                                       |
|--------------------------------|---------------------------------------|
| Port                           | : po30                                |
| Ifindex                        | : 4630                                |
| Port Status                    | : Up                                  |
| Port State                     | : Full                                |
| Last event                     | : AdjNodeLSEPresent                   |
| Port BPDU Receive Count        | : 132                                 |
| Adjacent Node Name             | : Building-A                          |
| Adjacent Ifindex               | : 4630                                |
| Adjacent MAC                   | : eccd.6daa.c861                      |
| Port Last Message Response     | : 0                                   |
| Link State Entries:            |                                       |
| Crosslink Ports Blocking       | : False                               |
| Node.Ifindex                   | : Building-A.4630 - Example-core.4630 |
| Transaction ID                 | : 2 - 2                               |
| MAC Address                    | : eccd.6daa.c861 - 0000.cd37.054b     |
| Link State                     | : Full - Full                         |
| Node.Ifindex                   | : Building-B.4610 - Example-core.4610 |
| Transaction ID                 | : 2 - 2                               |
| MAC Address                    | : eccd.6ddl.64d0 - 0000.cd37.054b     |
| Link State                     | : Full - Full                         |
| Domain Nodes Tree:             |                                       |
| Node                           | : Building-A                          |
| Links on Node                  | : 1                                   |
| Link 0                         | : Building-A.4630 - Example-core.4630 |
| Forwarding State               | : Forwarding                          |
| Node                           | : Building-B                          |
| Links on Node                  | : 1                                   |
| Link 0                         | : Building-B.4610 - Example-core.4610 |
| Forwarding State               | : Forwarding                          |
| Node                           | : Example-core                        |
| Links on Node                  | : 2                                   |
| Link 0                         | : Building-A.4630 - Example-core.4630 |
| Forwarding State               | : Forwarding                          |
| Link 1                         | : Building-B.4610 - Example-core.4610 |
| Forwarding State               | : Forwarding                          |
| Crosslink Transaction Entries: |                                       |
| Node                           | : Building-B                          |
| Transaction ID                 | : 2                                   |
| Uplink Transaction ID          | : 6                                   |
| Node                           | : Building-A                          |
| Transaction ID                 | : 2                                   |
| Uplink Transaction ID          | : 6                                   |
| Uplink Information:            |                                       |
| Waiting for Sync               | : 0                                   |
| Transaction ID                 | : 6                                   |
| Number of Links                | : 0                                   |
| Number of Local Uplinks        | : 0                                   |

**Table 43:** Sample output from the **show atmf links detail** command (cont.)

|                              |                   |
|------------------------------|-------------------|
| Originating Node             | : Building-A      |
| Domain                       | : -'s domain      |
| Node                         | : Building-A      |
| Ifindex                      | : 0               |
| Node Depth                   | : 0               |
| Transaction ID               | : 6               |
| Flags                        | : 32              |
| Domain Controller            | : -               |
| Domain Controller MAC        | : 0000.0000.0000  |
| Originating Node             | : Building-B      |
| Domain                       | : -'s domain      |
| Node                         | : Building-B      |
| Ifindex                      | : 0               |
| Node Depth                   | : 0               |
| Transaction ID               | : 6               |
| Flags                        | : 32              |
| Domain Controller            | : -               |
| Domain Controller MAC        | : 0000.0000.0000  |
| Downlink Domain Information: |                   |
| Domain                       | : Dept-A's domain |
| Domain Controller            | : Dept-A          |
| Domain Controller MAC        | : eccd.6d20.c1d9  |
| Number of Links              | : 2               |
| Number of Links Up           | : 2               |
| Number of Links on This Node | : 2               |
| Links are Blocked            | : 0               |
| Node Transaction List        |                   |
| Node                         | : Building-B      |
| Transaction ID               | : 8               |
| Node                         | : Building-A      |
| Transaction ID               | : 8               |
| Domain List                  |                   |
| Domain                       | : Dept-A's domain |
| Node                         | : Example-core    |
| Ifindex                      | : 4621            |
| Transaction ID               | : 8               |
| Flags                        | : 1               |
| Domain                       | : Dept-A's domain |
| Node                         | : Example-core    |
| Ifindex                      | : 4622            |
| Transaction ID               | : 8               |
| Flags                        | : 1               |

**Table 43:** Sample output from the **show atmf links detail** command (cont.)

|                              |                         |
|------------------------------|-------------------------|
| Domain                       | : Dorm-D's domain       |
| Domain Controller            | : Dorm-D                |
| Domain Controller MAC        | : 0000.cd37.082c        |
| Number of Links              | : 2                     |
| Number of Links Up           | : 2                     |
| Number of Links on This Node | : 2                     |
| Links are Blocked            | : 0                     |
| Node Transaction List        |                         |
| Node                         | : Building-B            |
| Transaction ID               | : 20                    |
| Node                         | : Building-A            |
| Transaction ID               | : 20                    |
| Domain List                  |                         |
| Domain                       | : Dorm-D's domain       |
| Node                         | : Building-A            |
| Ifindex                      | : 0                     |
| Transaction ID               | : 20                    |
| Flags                        | : 32                    |
| Domain                       | : Dorm-D's domain       |
| Node                         | : Building-B            |
| Ifindex                      | : 0                     |
| Transaction ID               | : 20                    |
| Flags                        | : 32                    |
| Domain                       | : Dorm-D's domain       |
| Node                         | : Example-core          |
| Ifindex                      | : 4510                  |
| Transaction ID               | : 20                    |
| Flags                        | : 1                     |
| Domain                       | : Dorm-D's domain       |
| Node                         | : Example-core          |
| Ifindex                      | : 4520                  |
| Transaction ID               | : 20                    |
| Flags                        | : 1                     |
| Domain                       | : Example-edge's domain |
| Domain Controller            | : Example-edge          |
| Domain Controller MAC        | : 001a.eb93.7aa6        |
| Number of Links              | : 1                     |
| Number of Links Up           | : 1                     |
| Number of Links on This Node | : 0                     |
| Links are Blocked            | : 0                     |
| Node Transaction List        |                         |
| Node                         | : Building-B            |
| Transaction ID               | : 9                     |
| Node                         | : Building-A            |
| Transaction ID               | : 9                     |

**Table 43:** Sample output from the **show atmf links detail** command (cont.)

|                                |                         |
|--------------------------------|-------------------------|
| Domain List                    |                         |
| Domain                         | : Example-edge's domain |
| Node                           | : Building-A            |
| Ifindex                        | : 0                     |
| Transaction ID                 | : 9                     |
| Flags                          | : 32                    |
| Domain                         | : Example-edge's domain |
| Node                           | : Building-B            |
| Ifindex                        | : 5027                  |
| Transaction ID                 | : 9                     |
| Flags                          | : 1                     |
| -----                          |                         |
| Up/Downlink Ports Information  |                         |
| -----                          |                         |
| Port                           | : sa10                  |
| Ifindex                        | : 4510                  |
| Port Status                    | : Up                    |
| Port State                     | : Full                  |
| Last event                     | : LinkComplete          |
| Adjacent Node                  | : Dorm-A                |
| Adjacent Internal ID           | : 211                   |
| Adjacent Ifindex               | : 4510                  |
| Adjacent Board ID              | : 387                   |
| Adjacent MAC                   | : eccd.6ddf.6cdf        |
| Adjacent Domain Controller     | : Dorm-D                |
| Adjacent Domain Controller MAC | : 0000.cd37.082c        |
| Port Forwarding State          | : Forwarding            |
| Port BPDU Receive Count        | : 95                    |
| Port Sequence Number           | : 11                    |
| Port Adjacent Sequence Number  | : 7                     |
| Port Last Message Response     | : 0                     |
| Port                           | : po21                  |
| Ifindex                        | : 4621                  |
| Port Status                    | : Up                    |
| Port State                     | : Full                  |
| Last event                     | : LinkComplete          |
| Adjacent Node                  | : Dept-A                |
| Adjacent Internal ID           | : 29                    |
| Adjacent Ifindex               | : 4621                  |
| Adjacent Board ID              | : 340                   |
| Adjacent MAC                   | : eccd.6d20.c1d9        |
| Adjacent Domain Controller     | : Dept-A                |
| Adjacent Domain Controller MAC | : eccd.6d20.c1d9        |
| Port Forwarding State          | : Forwarding            |
| Port BPDU Receive Count        | : 96                    |
| Port Sequence Number           | : 8                     |
| Port Adjacent Sequence Number  | : 9                     |
| Port Last Message Response     | : 0                     |
| Special Link Present           | : FALSE                 |

**Table 44:** Parameter definitions from the **show atmf links detail** command output

| Parameter                     | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Crosslink Ports Information   | <p>Show details of all Crosslink ports on this Node:</p> <ul style="list-style-type: none"> <li>Port - Name of the Port or static aggregation (sa&lt;*&gt;).</li> <li>Ifindex - Interface index for the crosslink port.</li> <li>VR ID - Virtual router id for the crosslink port.</li> <li>Port Status - Status of the local port on the Node as UP or DOWN.</li> <li>Port State - AMF State of the local port. <ul style="list-style-type: none"> <li>Init - Link is down.</li> <li>Hold - Link transitioned to up state, but waiting for hold period to ensure link is stable.</li> <li>Incompatible - Neighbor rejected the link because of inconsistency in AMF configurations.</li> <li>OneWay - Link is up and has waited the hold down period and now attempting to link to another unit in another domain</li> <li>Full - Link hello packets are sent and received from its neighbor with its own node id.</li> <li>Shutdown - Link has been shut down by user configuration.</li> </ul> </li> </ul> <p>Port BPDU Receive Count - The number of AMF protocol PDU's received.</p> <ul style="list-style-type: none"> <li>Adjacent Node Name - The name of the adjacent node connected to this node.</li> <li>Adjacent Ifindex - Adjacent AMF Node connected to this Node.</li> <li>Adjacent VR ID - Virtual router id of the adjacent node in the domain.</li> <li>Adjacent MAC - MAC address of the adjacent node in the domain.</li> <li>Port Last Message Response - Response from the remote neighbor to our AMF last hello packet.</li> </ul> |
| Link State Entries            | <p>Shows all the link state database entries:</p> <ul style="list-style-type: none"> <li>Node.Ifindex - Shows adjacent Node names and Interface index.</li> <li>Transaction ID - Shows transaction id of the current crosslink transaction.</li> <li>MAC Address - Shows adjacent Node MAC addresses.</li> <li>Link State - Shows AMF states of adjacent nodes on the link.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Domain Nodes Tree             | <p>Shows all the nodes in the domain:</p> <ul style="list-style-type: none"> <li>Node - Name of the node in the domain.</li> <li>Links on Node - Number of crosslinks on a vertex/node.</li> <li>Link no - Shows adjacent Node names and Interface index.</li> <li>Forwarding State - Shows state of AMF link Forwarding/Blocking.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Crosslink Transaction Entries | <p>Shows all the transaction entries:</p> <ul style="list-style-type: none"> <li>Node - Name of the AMF node.</li> <li>Transaction ID - transaction id of the node.</li> <li>Uplink Transaction ID - transaction id of the remote node.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

**Table 44:** Parameter definitions from the **show atmf links detail** command output (cont.)

| Parameter                   | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Uplink Information          | <p>Show all uplink entries.</p> <ul style="list-style-type: none"> <li>• Waiting for Sync - Flag if uplinks are currently waiting for synchronization.</li> <li>• Transaction ID - Shows transaction id of the local node.</li> <li>• Number of Links - Number of up downlinks in the domain.</li> <li>• Number of Local Uplinks - Number of uplinks on this node to the parent domain.</li> <li>• Originating Node - Node originating the uplink information.</li> <li>• Domain - Name of the parent uplink domain.</li> <li>• Node - Name of the node in the parent domain, that is connected to the current domain.</li> <li>• Ifindex - Interface index of the parent node's link to the current domain.</li> <li>• VR ID - Virtual router id of the parent node's link to the current domain.</li> <li>• Transaction ID - Transaction identifier for the neighbor in crosslink.</li> <li>• Flags - Used in domain messages to exchange the state:<br/> ATMF_DOMAIN_FLAG_DOWN = 0<br/> ATMF_DOMAIN_FLAG_UP = 1<br/> ATMF_DOMAIN_FLAG_BLOCK = 2<br/> ATMF_DOMAIN_FLAG_NOT_PRESENT = 4<br/> ATMF_DOMAIN_FLAG_NO_NODE = 8<br/> ATMF_DOMAIN_FLAG_NOT_ACTIVE_PARENT = 16<br/> ATMF_DOMAIN_FLAG_NOT_LINKS = 32<br/> ATMF_DOMAIN_FLAG_NO_CONFIG = 64</li> <li>• Domain Controller - Domain Controller in the uplink domain</li> <li>• Domain Controller MAC - MAC address of Domain Controller in uplink domain</li> </ul> |
| Downlink Domain Information | <p>Shows all the downlink entries:</p> <ul style="list-style-type: none"> <li>• Domain - Name of the downlink domain.</li> <li>• Domain Controller - Controller of the downlink domain.</li> <li>• Domain Controller MAC - MAC address of the domain controller.</li> <li>• Number of Links - Total number of links to this domain from the Node.</li> <li>• Number of Links Up - Total number of links that are in UP state.</li> <li>• Number of Links on This Node - Number of links terminating on this node.</li> <li>• Links are Blocked - 0 links are not blocked to the domain. 1 All links are blocked to the domain.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Table 44:** Parameter definitions from the **show atmf links detail** command output (cont.)

| Parameter                     | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Node Transaction List         | <p>List of transactions from this downlink domain node.</p> <ul style="list-style-type: none"> <li>Node - 0 links are not blocked to the domain. 1 All links are blocked to the domain.</li> <li>Transaction ID - Transaction id for this node.</li> <li>Domain List: Shows list of nodes in the current domain and their links to the downlink domain.:</li> <li>Domain - Domain name of the downlink node.</li> <li>Node - Name of the node in the current domain.</li> <li>Ifindex - Interface index for the link from the node to the downlink domain.</li> <li>Transaction ID - Transaction id of the node in the current domain.</li> <li>Flags - As mentioned above.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Up/Downlink Ports Information | <p>Shows all the configured up and down link ports on this node:</p> <ul style="list-style-type: none"> <li>Port - Name of the local port.</li> <li>Ifindex - Interface index of the local port.</li> <li>VR ID - Virtual router id for the local port.</li> <li>Port Status - Shows status of the local port on the Node as UP/DOWN.</li> <li>Port State - AMF state of the local port.</li> <li>Adjacent Node - nodename of the adjacent node.</li> <li>Adjacent Internal ID - Unique node identifier of the remote node.</li> <li>Adjacent Ifindex - Interface index for the port of adjacent AMF node.</li> <li>Adjacent Board ID - Product identifier for the adjacent node.</li> <li>Adjacent VR ID - Virtual router id for the port on adjacent AMF node.</li> <li>Adjacent MAC - MAC address for the port on adjacent AMF node.</li> <li>Adjacent Domain Controller - nodename of the Domain controller for Adjacent AMF node.</li> <li>Adjacent Domain Controller MAC - MAC address of the Domain controller for Adjacent AMF node.</li> <li>Port Forwarding State - Local port forwarding state Forwarding or Blocking.</li> <li>Port BPDU Receive Count - count of AMF protocol PDU's received.</li> <li>Port Sequence Number - hello sequence number, incremented every time the data in the hello packet changes.</li> <li>Port Adjacent Sequence Number - remote ends sequence number used to check if we need to process this packet or just note it arrived.</li> <li>Port Last Message Response - response from the remote neighbor to our last hello packet.</li> </ul> |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Related  
commands**    no debug all  
                 clear atmf links statistics  
                 show atmf



# show atmf links guest

**Overview** This command displays information about guest nodes visible to an AMF device.

**Syntax** `show atmf links guest [interface <interface-range>]`

| Parameter                      | Description                                                                |
|--------------------------------|----------------------------------------------------------------------------|
| interface<br><interface-range> | Select a specific range of ports to display information about guest nodes. |

**Default** With no parameters specified this command will display its standard output for all ports with guest nodes connected.

**Mode** User Exec/Privileged Exec

**Usage notes** Use this command to display the guest nodes connected to a single parent node. If you want to see a list of all the guests in the AMF network, use [show atmf guests](#).

**Example 1** To display information about AMF guests that are connectible from node1, use the command:

```
node1# show atmf links guest
```

**Output** Figure 42-27: Example output from **show atmf links guest**

| node1#sh atmf links guest    |              |            |        |                |                   |
|------------------------------|--------------|------------|--------|----------------|-------------------|
| Guest Link Information:      |              |            |        |                |                   |
| DC = Discovery configuration |              |            |        |                |                   |
| S = static D = dynamic       |              |            |        |                |                   |
| Local Port                   | Guest Class  | Model Type | MAC DC | Address        | IP / IPv6 Address |
| 1.0.1                        | -            | other      | D      | 0013.1a1e.4589 | 192.168.1.2       |
| 1.0.2                        | astra-phone  | other      | D      | 0008.5d10.7635 | 192.168.1.3       |
| 1.0.3                        | cisco-phone2 | other      | S      | -              | 192.168.2.1       |
| 1.0.4                        | panasonic... | other      | D      | 0800.239e.f1fe | 192.168.1.5       |

Table 42-1: Parameters in the output from **show atmf links guest**

| Parameter   | Description                                                                                                                |
|-------------|----------------------------------------------------------------------------------------------------------------------------|
| Local Port  | The port on the parent node that connects to the guest.                                                                    |
| Guest Class | The name of the ATMF guest-class that has been assigned to the guest node by the <a href="#">atmf guest-class</a> command. |

Table 42-1: Parameters in the output from **show atmf links guest** (cont.)

| Parameter         | Description                                                                                                                                                                                                                 |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Model Type        | The model type of the guest node, as entered by the <a href="#">modeltype</a> command. Can be one of the following: <ul style="list-style-type: none"><li>• alliedware</li><li>• aw+</li><li>• tq</li><li>• other</li></ul> |
| DC                | The discovery method as applied by the <a href="#">discovery</a> command. This can be either dynamic (D) or static (S).                                                                                                     |
| MAC Address       | The MAC address of the guest node.                                                                                                                                                                                          |
| IP / IPv6 Address | The IP address of the guest node.                                                                                                                                                                                           |

**Related commands**

- [atmf guest-class](#)
- [discovery](#)
- [http-enable](#)
- [username \(atmf-guest\)](#)
- [modeltype](#)
- [switchport atmf-guestlink](#)
- [show atmf backup guest](#)

# show atmf links guest detail

**Overview** This command displays detailed information about guest nodes visible to an AMF device.

**Syntax** `show atmf links guest detail [interface <interface-range>]`

| Parameter                                                      | Description                                                                |
|----------------------------------------------------------------|----------------------------------------------------------------------------|
| <code>interface</code><br><code>&lt;interface-range&gt;</code> | Select a specific range of ports to display information about guest nodes. |

**Mode** User Exec and Privileged Exec

**Usage notes** Use this command to display the guest nodes connected to a single parent node. If you want to see a list of all the guests in the AMF network, use [show atmf guests detail](#).

Note that the parameters that are displayed depend on the guest node's model and state.

**Example** To display detailed information about AMF guests, use the command:

```
node1# show atmf links guest detail
```

**Output** Figure 42-28: Example output from **show atmf links guest detail**

```

node1#show atmf links guest detail

Detailed Guest Link Information:

Interface : port1.0.13
Link State : Down
Class Name : test
Model Type : Other
Discovery Method : Static
IP Address : 192.168.1.13
Node State : Down

Interface : port1.0.5
Link State : Full
Class Name : tq_device
Model Type : TQ
Discovery Method : Dynamic
IP Address : 192.168.1.221
Username : manager
Login Fallback : Yes
Node State : Full
Backup Supported : Yes
MAC address : 001a.ebab.d2e0
Device Type : AT-TQ4600
Description : AP221
Firmware Version : 3.2.1 B02
HTTP port : 80

```

Table 42-2: Parameters in the output from **show atmf links guest detail**

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface  | The port on the parent node that connects to the guest.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Link State | <p>The state of the link to the guest node; one of:</p> <ul style="list-style-type: none"> <li>Down: The physical link is down.</li> <li>Up: The physical link has come up, but it is still during a timeout period that is enforced to allow other links to come up.</li> <li>Learn: The timeout period described above has elapsed, and the link is now learning information from the AMF guest node. You can see what information it is learning from the "Node State" field below.</li> <li>Full: The node connected by this link has joined the AMF network.</li> <li>Fail: The port is physically up but something has prevented the guest node from joining the AMF network.</li> </ul> |
| Class Name | The name of the ATMF guest-class that has been assigned to the guest node by the <b>atmf guest-class</b> command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 42-2: Parameters in the output from **show atmf links guest detail** (cont.)

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Model Type       | The model type of the guest node, as entered by the <a href="#">modeltype</a> command. The mode type can be one of the following: <ul style="list-style-type: none"> <li>alliedware</li> <li>aw+</li> <li>onvif</li> <li>tq</li> <li>other</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Discovery Method | The discovery method as applied by the <a href="#">discovery</a> command. This can be either dynamic or static.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| IP Address       | The IP address of the guest node.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Username         | The user name configured on the guest node.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Login Fallback   | Whether the guest node supports Login Fallback. For TQ model guest nodes, when login fallback is enabled, if a guest node is replaced, then AMF logs in to the new TQ using the factory default manager/friend settings. The new TQ is then discovered and managed as an AMF guest node by an AMF master or member. This means any backed up settings for the replaced guest node can also be recovered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Node state       | The state of the guest node; one of: <ul style="list-style-type: none"> <li>Down: The initial state when a link to a guest node is first configured. This is also the state if the physical link goes down.</li> <li>Getting IP: The AMF device is in the process of retrieving the IP address of the guest node.</li> <li>Getting Mac: The AMF device is in the process of retrieving the MAC address of the guest node.</li> <li>Getting Info: The AMF device is in the process of retrieving any other available information from the guest (firmware version etc). The information available depends on what device the guest node is.</li> <li>Full: The AMF device has retrieved all necessary information and the guest node has joined the AMF network. Once this state is reached, the Link State also changes to "Full".</li> <li>Failure: The physical link is up but the AMF member has failed to retrieve enough information to allow the guest node to join the AMF network.</li> </ul> |
| Backup Supported | Whether the guest node supports AMF backup functionality.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| MAC Address      | The MAC address of the guest node.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Table 42-2: Parameters in the output from **show atmf links guest detail** (cont.)

| Parameter        | Description                                                                                                                                                                                                                           |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Device Type      | Model information for the guest node. This field shows the model information that AMF retrieved from the guest node. In contrast, the Model Type shows what a user entered as the type of device they intended this guest node to be. |
| Description      | By default, this is a concatenation of the guest node's parent node and the port to which it is attached. You can change it by configuring a description on the port.                                                                 |
| Serial Number    | The serial number of the guest node.                                                                                                                                                                                                  |
| Firmware Name    | The name of the firmware operating on the guest node.                                                                                                                                                                                 |
| Firmware Version | The version of the firmware operating on the guest node.                                                                                                                                                                              |
| HTTP port        | The HTTP port as specified with the <a href="#">http-enable</a> command when defining a guest class. You can set this if the guest node provides an HTTP user interface on a non-standard port (any port other than port 80).         |

**Related  
commands**

[atmf guest-class](#)  
[discovery](#)  
[http-enable](#)  
[username \(atmf-guest\)](#)  
[modeltype](#)  
[switchport atmf-guestlink](#)  
[show atmf backup guest](#)

**Command  
changes**

Version 5.5.0-1.1: **Login Fallback** parameter added

# show atmf links statistics

**Overview** This command displays details of the AMF links configured on the device and also displays statistics about the AMF packet exchanges between the devices.

It is also possible to display the AMF link configuration and packet exchange statistics for a specified interface.

This command can only be run on AMF master and controller nodes

**Syntax** `show atmf links statistics [interface [<port-number>]]`

| Parameter     | Description                                                                                                                                                                                                              |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface     | Specifies that the command applies to a specific interface (port) or range of ports. Where both the interface and port number are unspecified, full statistics (not just those relating to ports) will be displayed.     |
| <port-number> | Enter the port number for which statistics are required. A port range, a static channel or LACP link can also be specified. Where no port number is specified, statistics will be displayed for all ports on the device. |

**Mode** User Exec

**Example 1** To display AMF link statistics for the whole device, use the command:

```
device1# show atmf links statistics
```

**Table 43:** Sample output from the **show atmf links statistics** command

|                        |         |          |
|------------------------|---------|----------|
| ATMF Statistics:       |         |          |
|                        | Receive | Transmit |
| -----                  |         |          |
| Arealink Hello         | 318     | 327      |
| Crosslink Hello        | 164     | 167      |
| Crosslink Hello Domain | 89      | 92       |
| Crosslink Hello Uplink | 86      | 88       |
| Hello Link             | 0       | 0        |
| Hello Neighbor         | 628     | 630      |
| Hello Stack            | 0       | 0        |
| Hello Gateway          | 1257    | 1257     |
| Database Description   | 28      | 28       |
| Database Request       | 8       | 6        |
| Database Update        | 66      | 162      |
| Database Update Bitmap | 0       | 29       |
| Database Acknowledge   | 144     | 51       |

**Table 43:** Sample output from the **show atmf links statistics** command (cont.)

| Transmit Fails                | 0       | 1                                                           |          |                  |
|-------------------------------|---------|-------------------------------------------------------------|----------|------------------|
| Discards                      | 0       | 0                                                           |          |                  |
| Total ATMF Packets            | 2788    | 2837                                                        |          |                  |
| ATMF Database Statistics:     |         |                                                             |          |                  |
| Database Entries              | 18      |                                                             |          |                  |
| Database Full Ages            | 0       |                                                             |          |                  |
| ATMF Virtual Link Statistics: |         |                                                             |          |                  |
| Virtual link                  | Receive | Receive Dropped                                             | Transmit | Transmit Dropped |
| -----                         |         |                                                             |          |                  |
| vlink2000                     | 393     | 0                                                           | 417      | 0                |
| ATMF Packet Discards:         |         |                                                             |          |                  |
| Type0                         | 0       | : Gateway hello msg received from unexpected neighbor       |          |                  |
| Type1                         | 0       | : Stack hello msg received from unexpected neighbor         |          |                  |
| Type2                         | 0       | : Discard TX update bitmap packet - bad checksum            |          |                  |
| Type3                         | 0       | : Discard TX update packet - neighbor not in correct state  |          |                  |
| Type4                         | 0       | : Discard update packet - bad checksum or type              |          |                  |
| Type5                         | 0       | : Discard update packet - neighbor not in correct state     |          |                  |
| Type6                         | 0       | : Discard update bitmap packet - bad checksum or type       |          |                  |
| Type7                         | 0       | : Incarnation is not possible with the data received        |          |                  |
| Type8                         | 0       | : Discard crosslink hello received - not correct state      |          |                  |
| Type9                         | 0       | : Discard crosslink domain hello received on non crosslink  |          |                  |
| Type10                        | 0       | : Discard crosslink domain hello - not in correct state     |          |                  |
| Type11                        | 0       | : Crosslink uplink hello received on non crosslink port     |          |                  |
| Type12                        | 0       | : Discard crosslink uplink hello - not in correct state     |          |                  |
| Type13                        | 0       | : Wrong network-name for this ATMF                          |          |                  |
| Type14                        | 0       | : Packet received on port is too long                       |          |                  |
| Type15                        | 0       | : Bad protocol version, received on port                    |          |                  |
| Type16                        | 0       | : Bad packet checksum calculation                           |          |                  |
| Type17                        | 0       | : Bad authentication type                                   |          |                  |
| Type18                        | 0       | : Bad simple password                                       |          |                  |
| Type19                        | 0       | : Unsupported authentication type                           |          |                  |
| Type20                        | 0       | : Discard packet - unknown neighbor                         |          |                  |
| Type21                        | 0       | : Discard packet - port is shutdown                         |          |                  |
| Type22                        | 0       | : Non broadcast hello msg received from unexpected neighbor |          |                  |
| Type23                        | 0       | : Arealink hello msg received on non arealink port          |          |                  |
| Type24                        | 0       | : Discard arealink hello packet - not in correct state      |          |                  |
| Type25                        | 0       | : Discard arealink hello packet - failed basic processing   |          |                  |
| Type26                        | 0       | : Discard unicast packet - MAC address does not match node  |          |                  |
| Type27                        | 0       | : AMF Master license node limit exceeded                    |          |                  |

**Example 2** To display the AMF links statistics on interface port1.0.4, use the command:

```
device1# show atmf links statistics interface port1.0.4
```



Figure 42-29: Sample output from the **show atmf links statistics** command for interface port1.0.4

```
device1# show atmf links statistics interface port1.0.4
```

| ATMF Port Statistics: |                        | Transmit | Receive |
|-----------------------|------------------------|----------|---------|
|                       |                        | -----    | -----   |
| port1.0.4             | Crosslink Hello        | 231      | 232     |
| port1.0.4             | Crosslink Hello Domain | 116      | 116     |
| port1.0.4             | Crosslink Hello Uplink | 116      | 115     |
| port1.0.4             | Hello Link             | 0        | 0       |
| port1.0.4             | Arealink Hello         | 0        | 0       |

Figure 42-30: Parameter definitions from the **show atmf links statistics** command output

| Parameter            | Definition                                                             |
|----------------------|------------------------------------------------------------------------|
| Receive              | Shows a count of AMF protocol packets received per message type.       |
| Transmit             | Shows the number of AMF protocol packets transmitted per message type. |
| Database Entries     | Shows the number of AMF elements existing in the distributed database. |
| Database Full Ages   | Shows the number of times the entries aged in the database.            |
| ATMF Packet Discards | Shows the number of discarded packets of each type.                    |

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Related commands**

- [no debug all](#)
- [clear atmf links statistics](#)
- [show atmf](#)

# show atmf nodes

**Overview** This command displays nodes currently configured within the AMF network.

Note that the output also tells you whether or not node map exchange is active. Node map exchange improves the tracking of nodes joining and leaving an AMF network. This improves the efficiency of AMF networks. Node map exchange is only available if every node in your AMF network is running version 5.4.6-2.1 or later. We recommend running the latest version on all nodes in your network, so you receive the advantages of node map exchange and other improvements.

**Syntax** `show atmf nodes [guest|all]`

| Parameter | Description                                                  |
|-----------|--------------------------------------------------------------|
| guest     | Display only guest nodes in the AMF network.                 |
| all       | Display all nodes in the AMF network, including guest nodes. |

**Mode** Privileged Exec

**Usage notes** You can use this command to display one of three sets of nodes:

- all nodes except guest nodes, by specifying **show atmf nodes**
- all nodes including guest nodes, by specifying **show atmf nodes all**
- only guest nodes, by specifying **show atmf nodes guest**

**Examples** To display AMF information for all nodes except guest nodes, use the command:

```
node1# show atmf nodes
```

Table 42-1: Sample output from **show atmf nodes**

|                                                |            |        |    |        |  |       |
|------------------------------------------------|------------|--------|----|--------|--|-------|
| node1#show atmf nodes guest                    |            |        |    |        |  |       |
| Node Information:                              |            |        |    |        |  |       |
| * = Local device                               |            |        |    |        |  |       |
| SC = Switch Configuration:                     |            |        |    |        |  |       |
| C = Chassis    S = Stackable    N = Standalone |            |        |    |        |  |       |
| Node                                           | Device     | ATMF   |    | Parent |  | Node  |
| Name                                           | Type       | Master | SC | Domain |  | Depth |
| -----                                          |            |        |    |        |  |       |
| * M1                                           | x510-28GTX | Y      | S  | none   |  | 0     |
| N3                                             | x230-18GP  | N      | N  | M1     |  | 1     |
| N1                                             | AR4050S    | N      | N  | M1     |  | 1     |
| Node map exchange is active                    |            |        |    |        |  |       |
| Current ATMF node count 3                      |            |        |    |        |  |       |

To display AMF information for all nodes, including guest nodes, use the command:

```
node1# show atmf nodes all
```

**Table 43:** Sample output from **show atmf nodes all**. In this example, not all nodes support node map exchange, as shown by the message at the end

```
node1#show atmf nodes all
```

Node and Guest Information:

\* = Local device

SC = Switch Configuration:  
C = Chassis S = Stackable N = Standalone G = Guest

| Node/Guest<br>Name | Device<br>Type | ATMF<br>Master | SC | Parent<br>Domain | Node<br>Depth |
|--------------------|----------------|----------------|----|------------------|---------------|
| * M1               | x510-28GTX     | Y              | S  | none             | 0             |
| N3                 | x230-18GP      | N              | N  | M1               | 1             |
| N1                 | AR4050S        | N              | N  | M1               | 1             |
| N3-1.0.24          | AT-TQ4600      | N              | G  | N3               | -             |

Node map exchange is inactive  
Firmware on some nodes does not support node map exchange, eg AR4050S  
Current ATMF node count 4 (guests 1)

To display AMF information for guest nodes only, use the command:

```
node1# show atmf nodes guest
```

**Table 42-1:** Sample output from **show atmf nodes guest**

```
node1#show atmf nodes guest
```

Guest Information:

| Device<br>Name | MAC<br>Address | Parent | Port  | IP/IPv6<br>Address |
|----------------|----------------|--------|-------|--------------------|
| aastra-...     | 0008.5d10.7635 | Node-1 | 1.0.2 | 192.168.4.7        |
| poe-1.0.1      | 0013.1a1e.4589 | Node-1 | 1.0.1 | 192.168.4.6        |
| ip-camera      | 0800.239e.f1fe | Node-1 | 1.0.4 | 192.168.4.8        |
| tq4600         | eccd.6df2.da60 | Node-1 | 1.0.5 | 192.168.4.50       |

**Related commands**

- [show atmf](#)
- [show atmf area nodes](#)
- [discovery](#)
- [http-enable](#)
- [show atmf backup guest](#)

# show atmf provision nodes

**Overview** This command displays information about each provisioned node with details about date and time of creation, boot and configuration files available in the backup, and license files present in the provisioned backup. This includes nodes that have joined the network but are yet to run their first backup.

This command can only be run on AMF master and controller nodes.

**Syntax** `show atmf provision nodes`

**Mode** Privileged Exec

**Usage notes** This command will only work if provisioned nodes have already been set up. Otherwise, an error message is shown when the command is run.

**Example** To show the details of all the provisioned nodes in the backup use the command:

```
NodeName# show atmf provision nodes
```

Figure 42-31: Sample output from the **show atmf provision nodes** command

```
device1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media: SD (Total 3827.0MB, Free 3481.1MB)

Node Name : device2
Date& Time : 06-Oct-2016 & 23:25:44
Provision Path : card:/atmf/provision_nodes

Boot configuration :
Current boot image : x510-5.4.9-0.1.rel (file exists)
Backup boot image : x510-5.4.8-2.3.rel (file exists)
Default boot config : flash:/default.cfg (file exists)
Current boot config : flash:/abc.cfg (file exists)
Backup boot config : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file : ../configs/.sw_v2.lic
 : ../configs/.swfeature.lic
Certificate file : card:/atmf/nodes/awplus1/flash/.atmf-lic-cert
```

**Related commands**

- [atmf provision \(interface\)](#)
- [atmf provision node](#)
- [clone \(amf-provision\)](#)
- [configure boot config \(amf-provision\)](#)
- [configure boot system \(amf-provision\)](#)
- [create \(amf-provision\)](#)

delete (amf-provision)  
identity (amf-provision)  
license-cert (amf-provision)  
locate (amf-provision)

# show atmf recovery-file

**Overview** Use this command to display the recovery file information for an AMF node.  
AMF recovery files are created for nodes with special links. Special links include:

- virtual links,
- area links terminating on an AMF master, and
- area virtual links terminating on an AMF master.

**Syntax** `show atmf recovery-file`

**Mode** Privileged Exec

**Example** To display recovery file information for an AMF node, use the command:

```
node1# show atmf recovery-file
```

**Output** Figure 42-32: Example output from **show atmf recovery-file**

```
node1#show atmf recovery-file

ATMF Recovery File Info: Special Link Present
Location Date Time
USB storage device 30 Apr 2018 14:50:32
Master 30 Apr 2018 14:56:45
node1 30 Apr 2018 14:56:45
node3 30 Apr 2018 14:56:45
```

**Related commands** [clear atmf recovery-file](#)  
[show atmf backup](#)

**Command changes** Version 5.4.8-0.2: command added

# show atmf secure-mode

**Overview** Use this command to display an overview of the secure mode status of an AMF network.

**Syntax** `show atmf secure-mode`

**Mode** Privileged Exec

**Example** To display an overview of AMF secure mode on an AMF master or member node, use the command:

```
awplus# show atmf secure-mode
```

**Output** Figure 42-33: Example output from **show atmf secure-mode** on an AMF master

```
ATMF Secure Mode:

Secure Mode Status : Enabled
Certificate Expiry : 180 Days
Certificates Total : 8
Certificates Revoked : 0
Certificates Rejected : 0
Certificates Active : 8

Provisional Authorization : 0
Pending Requests : 0

Trusted Master : master_1
Trusted Master : master_2

Key Fingerprint:
 48:37:d9:a0:37:32:22:9b:5c:22:da:a2:62:49:a7:e5:a9:bc:12:88
```

Figure 42-34: Example output from **show atmf secure-mode** on an AMF node

```
ATMF Secure Mode:

Secure Mode Status : Enabled
Trusted Master : master_1
Trusted Master : master_2

Key Fingerprint:
 93:f0:52:a9:74:8f:ae:ea:5b:e2:ee:62:cb:6b:21:22:5a:08:db:98
```

Table 42-2: Parameters in the output from **show atmf secure-mode**

| Parameter                 | Description                                                                                                                                        |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Secure Mode Status        | Shows the status of secure mode, Enabled or Disabled.                                                                                              |
| Certificate Expiry        | Certificate expiry time. Set with <a href="#">atmf secure-mode certificate expiry</a>                                                              |
| Certificates Total        | Total number of certificates.                                                                                                                      |
| Certificates Revoked      | Certificates that have been revoked by the AMF master.                                                                                             |
| Certificates Rejected     | Certificates that have been rejected by the AMF master.                                                                                            |
| Certificates Active       | Certificates that are currently active.                                                                                                            |
| Provisional Authorization | Number of nodes with provisional authorization. For more information use the <a href="#">show atmf authorization provisional</a> command.          |
| Pending Requests          | Number of nodes waiting for authorization on the AMF master. For more information use the <a href="#">show atmf authorization pending</a> command. |
| Trusted Master            | List of trusted masters in the AMF area.                                                                                                           |
| Key Fingerprint           | The AMF node's key fingerprint.                                                                                                                    |

**Related commands**

- [atmf authorize](#)
- [atmf secure-mode](#)
- [atmf secure-mode certificate expiry](#)
- [show atmf authorization](#)
- [show atmf secure-mode audit link](#)

**Command changes**

- Version 5.4.7-0.3: command added



# show atmf secure-mode audit

**Overview** Use this command to detect security vulnerabilities on a node.

**Syntax** show atmf secure-mode audit

**Mode** Privileged Exec

**Example** To display AMF secure mode link audits for a node, use the command

```
awplus# show atmf secure-mode audit
```

**Output** Figure 42-35: Example output from **show atmf secure-mode audit**

```
ATMF Secure Mode Audit:

Warning : The default username and password is enabled.
Good : SNMP V1 or V2 is disabled.
Warning : Telnet server is enabled.
Good : ATMF is enabled. Secure-Mode is on.
Good : ATMF Topology-GUI is disabled. No trustpoints configured.

ATMF Secure Mode Log Events:

2017 Feb 2 00:59:25 user.notice node1 ATMF[848]: Sec_Audit - ATMF Secure
Mode is enabled.
2017 Feb 2 01:30:00 user.notice node1 ATMF[848]: Sec_Audit - Established
secure connection to area_1_node_1 on interface vlink1.
```

Table 42-3: Parameters in the output from **show atmf secure-mode audit link**

| Parameter                   | Description                                                                                                                                                                                                     |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ATMF Secure Mode Audit      | A list of security recommendations to secure the AMF network. Items prefaced with <code>Warning</code> need to be fixed. In the sample above the default username and password, and telnet, should be disabled. |
| ATMF Secure Mode Log Events | A list of recorded secure mode log events.                                                                                                                                                                      |

**Related commands** [show atmf secure-mode](#)

**Command changes** Version 5.4.7-0.3: command added

# show atmf secure-mode audit link

**Overview** Use this command to detect security vulnerabilities by identifying devices that are connected to a secure mode node that are not in secure mode or are not authorized.

**Syntax** `show atmf secure-mode audit link`

**Mode** Privileged Exec

**Example** To display AMF secure mode link audits for a node, use the command  
`awplus# show atmf secure-mode audit link`

**Output** Figure 42-36: Example output from **show atmf secure-mode audit link**

```
ATMF Secure Mode Audit Link:

* ATMF links connected to devices which are not authorized
 or are not in secure-mode.

Port Link Type Discovered Node/Area Name

vlink1 Downlink 16/02/2017 09:28:22 Member3
```

Table 42-4: Parameters in the output from **show atmf secure-mode audit link**

| Parameter      | Description                         |
|----------------|-------------------------------------|
| Port           | Port name on local device.          |
| Link Type      | Link type.                          |
| Discovered     | Date discovered                     |
| Node/Area Name | Node or area name of remote device. |

**Related commands** [show atmf](#)  
[show atmf secure-mode](#)

**Command changes** Version 5.4.7-0.3: command added

# show atmf secure-mode certificates

**Overview** Use this command to display the certificate status details when secure mode is enabled on an AMF network.

**Syntax** `show atmf secure-mode certificates [detail] [area <area-name>]  
[node <node-name>]`

| Parameter   | Description                                                   |
|-------------|---------------------------------------------------------------|
| detail      | Display detailed certificate information.                     |
| area        | Specify an AMF area.                                          |
| <area-name> | The AMF area you want to see the certificate information for. |
| node        | Specify an AMF node.                                          |
| <node-name> | The AMF node you want to see information for.                 |

**Mode** Privileged Exec

**Example** To display AMF secure mode certificates on a master or member node, use the command:

```
awplus# show atmf secure-mode certificates
```

To display detailed information about AMF secure mode certificates for a node named "area\_2\_node\_1" in an area named "area-2", use the command:

```
awplus# show atmf secure-mode certificates detail area area-2
node area_2_node_1
```

**Output** Figure 42-37: Example output from **show atmf secure-mode certificates**

| Area-1 Certificates: |          |             |          |
|----------------------|----------|-------------|----------|
| Node Name            | Signer   | Expires     | Status   |
| -----                |          |             |          |
| area_1_node_1        | master_1 | 11 Mar 2017 | Active   |
|                      | master_2 | 4 Mar 2017  |          |
| area_1_node_2        | master_1 | 11 Mar 2017 | Revoked  |
|                      | master_2 | 4 Mar 2017  |          |
|                      |          |             |          |
| Area-2 Certificates: |          |             |          |
| Node Name            | Signer   | Expires     | Status   |
| -----                |          |             |          |
| area_2_node_1        | master_1 | 18 Mar 2017 | Active   |
| area_2_node_2        | master_1 | 18 Mar 2017 | Rejected |

Table 42-5: Parameters in the output from **show atmf secure-mode certificates**

| Parameter | Description                                                                                                                                                                                     |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Node Name | Name of AMF node the certificate was issued to.                                                                                                                                                 |
| Signer    | Name of AMF master that issued the certificate.                                                                                                                                                 |
| Expires   | Certificate expiry date.                                                                                                                                                                        |
| Status    | The status column will display <i>Active</i> before a member node is trusted, and can be accessed using AMF commands. Valid statuses are <i>Active</i> , <i>Revoked</i> , and <i>Rejected</i> . |

**Output** Figure 42-38: Example output from **show atmf secure-mode certificates detail area area-2 node area\_2\_node\_1**

|                             |                                                               |
|-----------------------------|---------------------------------------------------------------|
| Certificates Detail:        |                                                               |
| -----                       |                                                               |
| area_2_node_1 (area:area-2) |                                                               |
| MAC Address                 | : 0000.cd37.0003                                              |
| Status                      | : Active                                                      |
| Serial Number               | : A24SC8001                                                   |
| Product                     | : x510-28GTX                                                  |
| Key Fingerprint             | : cd:b4:c9:cd:7b:87:6a:30:98:25:d7:3c:89:8e:cb:74:e8:91:56:9d |
| Flags                       | : 00000011                                                    |
| Signer                      | : master_1                                                    |
| Expiry Date                 | : 18 Mar 2017 21:17:42                                        |

Table 42-6: Parameters in the output from **show atmf secure-mode certificates detail**

| Parameter       | Description                                                                                                                                                                              |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MAC Address     | MAC address of AMF node.                                                                                                                                                                 |
| Status          | The device status will show <i>Active</i> if a member node is trusted, and can be accessed using AMF commands. Valid statuses are <i>Active</i> , <i>Revoked</i> , and <i>Rejected</i> . |
| Serial Number   | Device serial number.                                                                                                                                                                    |
| Product         | Device product type.                                                                                                                                                                     |
| Key Fingerprint | AMF node key fingerprint.                                                                                                                                                                |
| Flags           | Internal AMF information.                                                                                                                                                                |
| Signer          | Name of AMF master that issued the certificate.                                                                                                                                          |
| Expiry Date     | Certificate expiry date.                                                                                                                                                                 |

**Related commands**

- [atmf authorize](#)
- [atmf secure-mode](#)
- [atmf secure-mode certificate expire](#)
- [atmf secure-mode certificate renew](#)
- [clear atmf secure-mode certificates](#)
- [show atmf secure-mode sa](#)

**Command changes**    Version 5.4.7-0.3: command added

# show atmf secure-mode sa

**Overview** Use this command to display the security associations on the network. This is the list of links and neighbors that are trusted.

**Syntax** `show atmf secure-mode sa [detail] [link|neighbor|broadcast]`

| Parameter | Description                                        |
|-----------|----------------------------------------------------|
| detail    | Display detailed security association information. |
| link      | Display security associations for type links.      |
| neighbor  | Display security associations for type neighbors.  |
| broadcast | Display security associations for type broadcast.  |

**Mode** Privileged Exec

**Example** To display an overview of AMF secure mode security associations on a master or member node, use the command:

```
awplus# show atmf secure-mode sa
```

To display a detailed overview of AMF secure mode neighbor security associations on a master or member node, use the command:

```
awplus# show atmf secure-mode sa detail neighbor
```

**Output** Figure 42-39: Example output from **show atmf secure-mode sa**

| ATMF Security Associations: |               |          |            |
|-----------------------------|---------------|----------|------------|
| Type                        | State         | ID       | Details    |
| -----                       |               |          |            |
| Neighbor Node               | Complete      | 175      | master_1   |
| Broadcast                   | Complete      | 4095     |            |
| CrossLink                   | Complete      | 4501     | sa1        |
| AreaLink                    | Cert Exchg    | 4511     | sa11       |
| Link                        | Complete      | 6009     | port1.2.9  |
| AreaLink                    | CA Exchg Init | 6013     | port1.2.13 |
| AreaLink                    | Cert Exchg    | 13001    | port1.9.1  |
| Link                        | CA Exchg Init | 16779521 | vlink3     |
| Neighbor Gateway            | Complete      | 83       | master_2   |
| Neighbor Gateway            | Complete      | 175      | master_1   |
| Neighbor Cntl-Master        | Complete      | 83       | master_2   |
| Neighbor Cntl-Master        | Complete      | 175      | master_1   |

Figure 42-40: Example output from **show atm secure-mode sa detail neighbor**

```
Security Associations Detail:

Id : 175 (af)
 Type : Neighbor Node
 State : Complete
 Remote MAC Address : eccd.6d82.6c16
 Flags : 000003c0

Id : 83 (40000053)
 Type : Neighbor Gateway
 State : Complete
 Remote MAC Address : 001a.eb54.e53b
 Flags : 000003c0

Id : 175 (400000af)
 Type : Neighbor Gateway
 State : Complete
 Remote MAC Address : eccd.6d82.6c16
 Flags : 000003c0

Id : 83 (80000053)
 Type : Neighbor Cntl-Master
 State : Complete
 Remote MAC Address : 001a.eb54.e53b
 Flags : 000003c0

Id : 175 (800000af)
 Type : Neighbor Cntl-Master
 State : Complete
 Remote MAC Address : eccd.6d82.6c16
 Flags : 000003c0

Id : 321 (80000141)
 Type : Neighbor Cntl-Master
 State : Complete
 Remote MAC Address : 0000.f427.93da
 Flags : 000003c0
```

Table 42-7: Parameters in the output from **show atmf secure-mode sa**

| Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type               | Security Association (SA) types: <ul style="list-style-type: none"><li>• Link - SA for link</li><li>• CrossLink - SA for crosslink</li><li>• AreaLink - SA for area link</li><li>• Neighbor Node - SA for node neighbor relationship</li><li>• Neighbor Gateway - SA for gateway neighbor relationship</li><li>• Neighbor Cntl-Master - SA for controller/master neighbor relationship</li><li>• Broadcast - SA for working-set broadcast requests</li></ul>                                                 |
| State              | Current state of the Security Association. The state must be <code>Complete</code> before a member node is trusted, and can be accessed using AMF commands. <ul style="list-style-type: none"><li>• CA Exchg Init - SA is ready to begin the SA exchange process</li><li>• CA Exchg - SA is currently exchanging CAs</li><li>• Cert Exchg - SA is currently exchanging certificates</li><li>• Key Exchg - SA is currently exchanging ephemeral keys</li><li>• Complete - SA exchange has completed</li></ul> |
| ID                 | Security Association ID. <ul style="list-style-type: none"><li>• For Neighbor types this is the remote node ID.</li><li>• For Link types this is the local ifindex.</li><li>• For Broadcast type this is always 4095.</li></ul>                                                                                                                                                                                                                                                                              |
| Details            | Human readable translation of ID. <ul style="list-style-type: none"><li>• For Neighbor types this is the node name</li><li>• For Link types this is the interface name</li></ul>                                                                                                                                                                                                                                                                                                                             |
| Remote MAC Address | MAC address of the remote partner of the security association.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Flags              | Internal AMF information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Related commands** [atmf secure-mode](#)  
[show atmf secure-mode](#)  
[show atmf secure-mode certificates](#)

**Command changes** Version 5.4.7-0.3: command added



# show atmf secure-mode statistics

**Overview** Use this command to display AMF secure mode statistics. These statistics are from when AMF secure mode was first enabled or the statistics were cleared with the [clear atmf secure-mode statistics](#) command.

**Syntax** show atmf secure-mode statistics

**Mode** Privileged Exec

**Example** To display AMF secure mode statistics on a master or member node, use the command:

```
awplus# show atmf secure-mode statistics
```

**Output** Figure 42-41: Example output from **show atmf secure-mode statistics** on an AMF master.

```
ATMF Secure Mode Statistics:

Certificates:
New 7 Expired 0
Updated 7 Deleted 0
Revoked 1 Renewed 2
Rejected 1 Re-authorized 1
Authorized 0

Local Certificates:
Valid 4 Invalid 0
Certificates Validation:
Request Valid 2
Request Invalid 0
Common Valid 13
Common Invalid 0
Issuer Valid 14
Issuer Invalid 0
Signature Verified 29
Signature Invalid 0
Signature Purpose Invalid 0

Signatures Signed 12
Master Certificates:
Re-issued 3
Downgraded to member 0

Public key change 2
Invalid SA public key 0
```

**Output** Figure 42-42: Example output from **show atmf secure-mode statistics** on an AMF node.

```
ATMF Secure Mode Statistics:

Local Certificates:
Valid 3 Invalid 0

Certificates Validation:
Request Valid 0
Request Invalid 0
Common Valid 0
Common Invalid 0
Issuer Valid 12
Issuer Invalid 0
Signature Verified 12
Signature Invalid 3
Signature Purpose Invalid 0

Signatures Signed 0

Master Certificates:
Re-issued 0
Downgraded to member 0

Public key change 2
Invalid SA public key 0
```

**Related commands**

- [atmf authorize](#)
- [atmf secure-mode](#)
- [atmf secure-mode certificate renew](#)
- [clear atmf secure-mode statistics](#)
- [show atmf secure-mode](#)

**Command changes** Version 5.4.7-0.3: command added

# show atmf tech

**Overview** This command collects and displays all the AMF command output. The command can thus be used to display a complete picture of an AMF network.

**Syntax** show atmf tech

**Mode** Privileged Exec

**Example** To display output for all AMF commands, use the command:

```
NodeName# show atmf tech
```

**Table 43:** Sample output from the **show atmf tech** command.

```
node1#show atmf tech
ATMF Summary Information:

ATMF Status : Enabled
Network Name : ATMF_NET
Node Name : node1
Role : Master
Current ATMF Nodes : 8

ATMF Technical information:

Network Name : ATMF_NET
Domain : node1's domain
Node Depth : 0
Domain Flags : 0
Authentication Type : 0
MAC Address : 0014.2299.137d
Board ID : 287
Domain State : DomainController
Domain Controller : node1
Backup Domain Controller : node2
Domain controller MAC : 0014.2299.137d
Parent Domain : -
Parent Domain Controller : -
Parent Domain Controller MAC : 0000.0000.0000
Number of Domain Events : 0
Crosslink Ports Blocking : 0
Uplink Ports Waiting on Sync : 0
```

**Table 43:** Sample output from the **show atmf tech** command. (cont.)

|                                   |         |
|-----------------------------------|---------|
| Crosslink Sequence Number         | : 7     |
| Domains Sequence Number           | : 28    |
| Uplink Sequence Number            | : 2     |
| Number of Crosslink Ports         | : 1     |
| Number of Domain Nodes            | : 2     |
| Number of Neighbors               | : 5     |
| Number of Non Broadcast Neighbors | : 3     |
| Number of Link State Entries      | : 1     |
| Number of Up Uplinks              | : 0     |
| Number of Up Uplinks on This Node | : 0     |
| DBE Checksum                      | : 84fc6 |
| Number of DBE Entries             | : 0     |
| ...                               |         |

**Table 44:** Parameter definitions from the **show atmf tech** command

| Parameter          | Definition                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ATMF Status        | Shows status of AMF feature on the Node as Enabled/Disabled.                                                                                                                                                                                                                                                                                                                                         |
| Network Name       | The name of the AMF network to which this node belongs.                                                                                                                                                                                                                                                                                                                                              |
| Node Name          | The name assigned to the node within the AMF network.                                                                                                                                                                                                                                                                                                                                                |
| Role               | The role configured on the device within the AMF - either master or member.                                                                                                                                                                                                                                                                                                                          |
| Current ATMF Nodes | A count of the AMF nodes in the AMF network.                                                                                                                                                                                                                                                                                                                                                         |
| Node Address       | The identity of a node (in the format name.atmf) that enables its access it from a remote location.                                                                                                                                                                                                                                                                                                  |
| Node ID            | A unique identifier assigned to an AMF node.                                                                                                                                                                                                                                                                                                                                                         |
| Node Depth         | The number of nodes in the path from this node to the core domain.                                                                                                                                                                                                                                                                                                                                   |
| Domain State       | A node's state within an AMF Domain - either controller or backup.                                                                                                                                                                                                                                                                                                                                   |
| Recovery State     | The AMF node recovery status. Indicates whether a node recovery is in progress on this device - either Auto, Manual, or None.                                                                                                                                                                                                                                                                        |
| Management VLAN    | The VLAN created for traffic between nodes of different domains (up/down links).<br>VLAN ID - In this example VLAN 4092 is configured as the Management VLAN.<br>Management Subnet - the Network prefix for the subnet.<br>Management IP Address - the IP address allocated for this traffic.<br>Management Mask - the Netmask used to create a subnet for this traffic 255.255.128.0 (= prefix /17) |

**Table 44:** Parameter definitions from the **show atmf tech** command (cont.)

| Parameter   | Definition                                                                                                                                                                                                                                                                                                                                                                            |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain VLAN | The VLAN assigned for traffic between Nodes of same domain (crosslink).<br>VLAN ID - In this example VLAN 4091 is configured as the domain VLAN.<br>Domain Subnet - the Subnet address used for this traffic.<br>Domain IP Address - the IP address allocated for this traffic.<br>Domain Mask - the Netmask used to create a subnet for this traffic 255.255.128.0<br>(= prefix /17) |
| Device Type | Shows the Product Series Name.                                                                                                                                                                                                                                                                                                                                                        |
| ATMF Master | Indicates the node's membership of the core domain (membership is indicated by Y)                                                                                                                                                                                                                                                                                                     |
| SC          | Shows switch configuration: <ul style="list-style-type: none"><li>• C - Chassis (such as SBx8100 series)</li><li>• S - Stackable (VCS)</li><li>• N - Standalone</li></ul>                                                                                                                                                                                                             |
| Parent      | A node that is connected to the present node's uplink, i.e. one layer higher in the hierarchy.                                                                                                                                                                                                                                                                                        |
| Node Depth  | Shows the number of nodes in path from the current node to the Core domain.                                                                                                                                                                                                                                                                                                           |

**NOTE:** The **show atmf tech** command can produce very large output. For this reason only the most significant terms are defined in this table.

# show atmf virtual-links

**Overview** This command displays a summary of all virtual links (L2TP tunnels) currently in the running configuration.

**Syntax** `show atmf virtual-links [macaddr]`  
`show atmf virtual-links [id <1-4094>] [remote-id <1-4094>]`  
`show atmf virtual-links detail [id <1-4094>]`

| Parameter          | Description                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| macaddr            | Display the virtual AMF links' MAC addresses.                                                                                                                                              |
| id <1-4094>        | ID of the local virtual link.                                                                                                                                                              |
| remote-id <1-4094> | ID of the remote virtual link                                                                                                                                                              |
| detail             | Display information about a specific virtual link ID or range of virtual link IDs. Displays information such as: local and remote IP address, link type, packets received and transmitted. |

**Mode** Privileged Exec

**Example 1** To display AMF virtual links, use the command:

```
node_1# show atmf virtual-links
```

Table 42-1: Example output from **show atmf virtual-links**

| ATMF Virtual-Link Information: |          |              |           |              |                |              |
|--------------------------------|----------|--------------|-----------|--------------|----------------|--------------|
| Local Port                     | Local ID | Local IP     | Remote ID | Remote IP    | Tunnel Protect | Tunnel State |
| vlink1                         | 1        | 172.16.24.2  | 2         | 1.0.0.2      | -              | Complete     |
| vlink2                         | 2        | 172.16.24.2* | 10        | 172.16.24.3* | ipsec          | Complete     |
| vlink3                         | 3        | (eth0)*      | 1         | 1.2.3.4      | -              | AcquireLocal |
| * = Dynamic Address.           |          |              |           |              |                |              |
| Virtual Links Configured: 3    |          |              |           |              |                |              |

In the above example, a centrally located switch has the IP address space 192.0.2.x/24. It has two VLANs assigned the subnets 192.0.2.33 and 192.0.2.65 using the prefix /27. Each subnet connects to a virtual link. The first link has the IP address 192.168.1.1 and has a Local ID of 1. The second has the IP address 192.168.2.1 and has the Local ID of 2.

**Example 2** To display details about AMF virtual link with ID 1, use the command:

```
node_1# show atmf virtual-links detail id 1
```

Table 42-2: Example output from **show atmf virtual-links**

| Virtual Link Detailed Information: |                     |                |
|------------------------------------|---------------------|----------------|
| ID 1                               | Description         | : None         |
| ID 1                               | Local IP Address    | : 192.168.5.1  |
| ID 1                               | Remote ID           | : 1            |
| ID 1                               | Remote IP Address   | : 192.168.5.20 |
| ID 1                               | Link Type           | : virtual-link |
| ID 1                               | Packets Received    | : 236465       |
| ID 1                               | Packets Transmitted | : 192626       |

**Example 3** To display AMF virtual links' MAC address information, use the command:

```
node_1# show atmf virtual-links macaddr
```

Table 42-3: Example output from **show atmf virtual-links macaddr**

| ATMF Link Remote Information:       |                   |           |              |
|-------------------------------------|-------------------|-----------|--------------|
| ATMF Management Bridge Information: |                   |           |              |
| Bridge: br-atmfmgmt                 |                   |           |              |
| port no                             | mac addr          | is local? | ageing timer |
| 1                                   | 00:00:cd:27:c2:07 | yes       | 0.00         |
| 2                                   | 8e:c7:ae:81:7e:68 | yes       | 0.00         |
| 2                                   | 00:00:cd:28:bf:e7 | no        | 0.01         |

Table 42-4: Parameters in the output from **show atmf virtual-links**

| Parameter      | Definition                                                                                                                                 |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Local Port     | The tunnel name e.g. vlink1, vlink2, equivalent to an L2TP tunnel.                                                                         |
| Local ID       | The local ID of the virtual link. This matches the vlink<number>                                                                           |
| Tunnel Protect | Tunnel protection protocol.                                                                                                                |
| Tunnel State   | The operational state of the vlink (either Up or Down). This state is always displayed once a vlink has been created.                      |
| mac addr       | AMF virtual links terminate on an internal soft bridge. The "show atmf virtual-links macaddress" command displays MAC Address information. |
| is local?      | Indicates whether the MAC displayed is for a local or a remote device.                                                                     |
| ageing timer   | Indicates the current aging state for each MAC address.                                                                                    |

**Related commands** [atmf virtual-link](#)

# show atmf working-set

**Overview** This command displays the nodes that form the current AMF working-set.

**Syntax** `show atmf working-set`

**Mode** Privileged Exec

**Example** To show current members of the working-set, use the command:

```
ATMF_NETWORK[6]# show atmf working-set
```

**Table 43:** Sample output from the **show atmf working-set** command.

```
ATMF Working Set Nodes:

node1, node2, node3, node4, node5, node6

Working set contains 6 nodes
```

**Related commands**

- [atmf working-set](#)
- [show atmf](#)
- [show atmf group](#)



# show debugging atmf

**Overview** Use this command to see what debugging is turned on for AMF.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show debugging atmf

**Mode** Privileged Exec

**Example** To display the AMF debugging status, use the command:

```
node_1# show debugging atmf
```

Table 42-1: Sample output from the **show debugging atmf** command.

```
node_1# show debugging atmf
ATMF debugging status:
ATMF arealink debugging is on
ATMF link debugging is on
ATMF crosslink debugging is on
ATMF database debugging is on
ATMF neighbor debugging is on
ATMF packet debugging is on
ATMF error debugging is on
```

**Related commands** [debug atmf packet](#)

# show debugging atmf packet

**Overview** Use this command to see what debugging is turned on for AMF Packet debug.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show debugging atmf packet`

**Mode** User Exec and Privileged Exec

**Example** To display the AMF packet debugging status, use the command:

```
node_1# show debug atmf packet
```

Table 42-2: Sample output from the **show debugging atmf packet** command.

```
ATMF packet debugging is on
=== ATMF Packet Debugging Parameters===
Node Name: x908
Port name: port1.1.1
Limit: 500 packets
Direction: TX
Info Level: Level 2
Packet Type Bitmap:
2. Crosslink Hello BPDU pkt with downlink domain info
3. Crosslink Hello BPDU pkt with uplink info
4. Down and up link Hello BPDU pkts
6. Stack hello unicast pkts
8. DBE request
9. DBE update
10. DBE bitmap update
```

**Related commands** [debug atmf](#)  
[debug atmf packet](#)

# show running-config atmf

**Overview** This command displays the running system information that is specific to AMF.

**Syntax** `show running-config atmf`

**Mode** User Exec and Global Configuration

**Example** To display the current configuration of AMF, use the following commands:

```
node_1# show running-config atmf
```

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Related commands** `show running-config`  
`no debug all`

# state

**Overview** This command sets the running state of an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the [AMF Feature Overview and Configuration Guide](#) for more information on running multiple tenants on a single VAA host.

**Syntax** `state {enable|disable}`

| Parameter | Description                                                        |
|-----------|--------------------------------------------------------------------|
| disable   | Stop the AMF container. The container's state changes to stopped.  |
| enable    | Start the AMF container. The container's state changes to running. |

**Default** By default, **state** is disabled.

**Mode** AMF Container Configuration

**Usage notes** The first time the **state enable** command is executed on a container it assigns the container to an area and configures it as an AMF master. This is achieved by automatically adding the following configuration to the AMF container:

```
atmf network-name <AMF network-name>
atmf master
atmf area <container area-name> <container area-id> local
atmf area <container area-name> password <container area-password>
atmf area <host area-name> <host area-id>

interface eth0
 atmf-arealink remote-area <host area-name> vlan 4094
```

For this reason the **state enable** command should be run after the container has been created with the [atmf container](#) command and an area-link configured with the [area-link](#) command.

Once the start-up configuration has been saved from within the AMF container, all further configuration changes need to be made manually.

**Example** To start the AMF container “vac-wlg-1” use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# state enable
```

To stop the AMF container “vac-wlg-1” use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# state disable
```

**Related commands** [atmf container](#)  
[show atmf container](#)

**Command changes** Version 5.4.7-0.1: command added

# switchport atmf-agentlink

**Overview** Use this command to configure a link between this device and an x600 Series switch, in order to integrate the x600 Series switch into your AMF network. The x600 Series switch is called an “AMF agent”, and the link between the x600 and this device is called an “agent link”.

The x600 Series switch must be running version 5.4.2-3.16 or later.

Use the **no** variant of this command to remove the agent link. If the x600 Series switch is still connected to the switch port, it will no longer be part of the AMF network.

**Syntax** `switchport atmf-agentlink`  
`no switchport atmf-agentlink`

**Default** By default, no agent links exist and x600 Series switches are not visible to AMF networks.

**Mode** Interface mode for a switch port. Note that the link between the x600 and the AMF network must be a single link, not an aggregated link.

**Usage notes** The x600 Series switch provides the following information to the AMF node that it is connected to:

- The MAC address
- The IPv4 address
- The IPv6 address
- The name/type of the device (Allied Telesis x600)
- The name of the current firmware
- The version of the current firmware
- The configuration name

AMF guestnode also makes most of this information available from x600 Series switches, but requires configuration with DHCP and/or LLDP. AMF agent is simpler; as soon the x600 is connected to an appropriately configured port of an AMF node, it is immediately integrated into the AMF network.

To see information about the x600 Series switch, use the **show atmf links guest detail** command.

**Example** To configure port1.0.1 as an agent link, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport atmf-agentlink
```

**Related commands** [show atmf links guest](#)

# switchport atmf-arealink

**Overview** This command enables you to configure a port or aggregator to be an AMF area link. AMF area links are designed to operate between two nodes in different areas in an AMF network.

Use the **no** variant of this command to remove any AMF area link that may exist for the selected port or aggregated link.

This command is only available on AMF controllers and master nodes.

**Syntax** `switchport atmf-arealink remote-area <area-name> vlan <2-4094>`  
`no switchport atmf-arealink`

| Parameter   | Description                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <area-name> | The name of the remote area that the port is connecting to.                                                                          |
| <2-4094>    | The VLAN ID for the link. This VLAN cannot be used for any other purpose, and the same VLAN ID must be used at each end of the link. |

**Default** No arealinks are configured.

**Mode** Interface Configuration for a switchport, a static aggregator, or a dynamic channel group.

**Usage notes** Run this command on the port or aggregator at both ends of the link.  
Each area must have the area-name configured, and the same area password must exist on both ends of the link.

Running this command will automatically place the port or static aggregator into trunk mode (i.e. switchport mode trunk) and will synchronize the area information stored on the two nodes.

You can configure multiple arealinks between two area nodes, but only one arealink at any time will be in use. All other arealinks will block information, to prevent network storms.

**NOTE:** See the [atmf-arealink](#) command to configure an AMF area link on an AR-series Eth interface.

**Example** To make switchport port1.0.2 an arealink to the 'Auckland' area on VLAN 6, use the commands:

```
controller-1# configure terminal
controller-1(config)# interface port1.0.2
controller-1(config-if)# switchport atmf-arealink remote-area
Auckland vlan 6
```

To remove switchport port1.0.1 as an AMF area link, use the commands:

```
controller-1# configure terminal
controller-1(config)# interface port1.0.1
controller-1(config-if)# no switchport atmf-arealink
```

**Related  
commands**

[atmf area](#)  
[atmf area password](#)  
[atmf virtual-link](#)  
[show atmf links](#)



# switchport atmf-crosslink

**Overview** This command configures the selected port, statically aggregated link or dynamic channel group (LACP) to be an AMF crosslink. Running this command will automatically place the port or aggregator into trunk mode (i.e. **switchport mode trunk**).

The connection between two AMF masters must utilize a crosslink. Crosslinks are used to carry the AMF control information between master nodes. Multiple crosslinks can be configured between two master nodes, but only one crosslink can be active at any particular time. All other crosslinks between masters will be placed in the blocking state, in order to prevent broadcast storms.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove any crosslink that may exist for the selected port or aggregated link.

**Syntax** `switchport atmf-crosslink`  
`no switchport atmf-crosslink`

**Mode** Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

**Usage notes** Crosslinks can be used anywhere within an AMF network. They have the effect of separating the AMF network into separate domains.

Where this command is used, it is also good practice to use the **switchport trunk native vlan** command with the parameter **none** selected. This is to prevent a network storm on a topology of ring connected devices.

**Example 1** To make switchport port1.0.1 an AMF crosslink, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-crosslink
```

**Example 2** This example is shown twice. Example 2A is the most basic command sequence. Example 2B is a good practice equivalent that avoids problems such as broadcast storms that can otherwise occur.

**Example 2A** To make static aggregator sa1 an AMF crosslink, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface sa1
Node_1(config-if)# switchport atmf-crosslink
```

**Example 2B** To make static aggregator sa1 an AMF crosslink, use the following commands for good practice:

```
Node_1# configure terminal
Node_1(config)# interface sa1
Node_1(config-if)# switchport atmf-crosslink
Node_1(config-if)# switchport trunk allowed vlan add 2
Node_1(config-if)# switchport trunk native vlan none
```

In this example VLAN 2 is assigned to the static aggregator, and the native VLAN (VLAN 1) is explicitly excluded from the aggregated ports and the crosslink assigned to it.

**NOTE:** *The AMF management and domain VLANs are automatically added to the aggregator and the crosslink.*

**Related commands** [show atmf links statistics](#)

# switchport atmf-guestlink

**Overview** Guest links are used to provide basic AMF functionality to non AMF capable devices. Guest links can be configured for either a selected switch port or a range of switch ports and use generic protocols to collect status and configuration information that the guest devices make available.

Use the **no** variant of this command to remove the guest node functionality from the selected port or ports.

**NOTE:** AMF guest nodes are not supported on ports using the OpenFlow protocol.

**Syntax** `switchport atmf-guestlink [class <guest-class>] [ip <A.B.C.D> |  
ipv6 <X:X::X:X>]`  
`no switchport atmf-guestlink`

| Parameter     | Description                                                   |
|---------------|---------------------------------------------------------------|
| class         | Set a guest class                                             |
| <guest-class> | The name of the guest class.                                  |
| ip            | Specifies that the address following will have an IPv4 format |
| <A.B.C.D>     | The guest node's IP address in IPv4 format.                   |
| ipv6          | Specifies that the address following will have an IPv6 format |
| <X:X::X:X>    | The guest node's IP address in IPv6 format.                   |

**Default** No guest links are configured.

**Mode** Interface

**Example 1** To configure switchport port1.0.1 to be a guest link, that will connect to a guest node having a guest class of **camera** and an IPv4 address of **192.168.3.3**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink class camera ip
192.168.3.3
```

**Example 2** To configure switchport port1.0.1 to be a guest link, which will connect to a guest node having a guest class of **phone** and an IPv6 address of **2001:db8:21e:10d::5**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink class phone ipv6
2000:db8:21e:10d::5
```

**Example 3** To configure switchport port1.0.1 to be a guest link, using the default model type and learning method address, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink
```

**Example 4** To configure switchports port1.0.1 to port1.0.3 to be guest links, for the guest class **camera**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1-port1.0.3
node1(config-if)# switchport atmf-guestlink class camera
```

**Example 5** To remove the guest-link functionality from switchport port1.0.1, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# no switchport atmf-guestlink
```

**Related commands**

- [atmf guest-class](#)
- [discovery](#)
- [http-enable](#)
- [username \(atmf-guest\)](#)
- [modeltype](#)
- [show atmf links guest](#)
- [show atmf guests](#)

# switchport atmf-link

**Overview** This command enables you to configure a port or aggregator to be an up/down AMF link. Running this command will automatically place the port or aggregator into trunk mode. If the port was previously configured in access mode, the configured access VLAN will be removed.

Use the **no** variant of this command to remove any AMF link that may exist for the selected port or aggregated link.

**Syntax** `switchport atmf-link`  
`no switchport atmf-link`

**Mode** Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

**Usage notes** Up/down links and virtual links interconnect domains in a vertical hierarchy, with the highest domain being the core domain. In effect, they form a tree of interconnected AMF domains. This tree must be loop-free. Therefore you must configure your up/down and virtual links so that no loops are formed.

Within each domain, cross-links between AMF nodes define those nodes as siblings within the same domain. You can form rings by combining cross-links with up/down links and/or virtual links, as long as each AMF domain links upwards to only a single parent domain. Each domain may link downwards to multiple child domains.

**NOTE:** See the [atmf-link](#) command to configure an AMF up/down link on an AR-series Eth interface.

**Example** To configure switchport port1.0.1 as an AMF up/down link, use the commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-link
```

To remove switchport port1.0.1 as an AMF up/down link, use the commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# no switchport atmf-link
```

**Related commands** [atmf-link](#)  
[show atmf detail](#)  
[show atmf links](#)

# type atmf guest

**Overview** This command configures a trigger to activate when an AMF guest node joins or leaves.

**Syntax** `type atmf guest {join|leave}`

| Parameter | Description            |
|-----------|------------------------|
| join      | AMF guest node joins.  |
| leave     | AMF guest node leaves. |

**Mode** Trigger Configuration

**Example** To configure trigger 86 to activate when an AMF guest node leaves, use the following commands:

```
awplus(config)# trigger 86
awplus(config-trigger)# type atmf guest leave
```

**Related commands** [show trigger](#)

**Command changes** Version 5.5.1-1.1: command added

# type atmf node

**Overview** This command configures a trigger to activate when an AMF node joins or leaves.

**Syntax** type atmf node {join|leave}

| Parameter | Description      |
|-----------|------------------|
| join      | AMF node joins.  |
| leave     | AMF node leaves. |

**Mode** Trigger Configuration

**Example 1** To configure trigger 5 to activate when an AMF node leaves, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger)# type atmf node leave
```

**Example 2** The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
=====
node1, node2, node3:
=====

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

### Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=====
node1:
=====
```

| TR# | Type & Details    | Description         | Ac | Te | Tr | Repeat     | #Scr | Days/Date |
|-----|-------------------|---------------------|----|----|----|------------|------|-----------|
| 001 | Periodic (2 min)  | Periodic Status Chk | Y  | N  | Y  | Continuous | 1    | smtwtfs   |
| 005 | ATMF node (leave) | E-mail on ATMF Exit | Y  | N  | Y  | Continuous | 1    | smtwtfs   |

```

=====
Node2, Node3,
=====
```

| TR# | Type & Details    | Description         | Ac | Te | Tr | Repeat     | #Scr | Days/Date |
|-----|-------------------|---------------------|----|----|----|------------|------|-----------|
| 005 | ATMF node (leave) | E-mail on ATMF Exit | Y  | N  | Y  | Continuous | 1    | smtwtfs   |

```

```

### Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
=====
Node1:
=====

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!

=====
Node2, Node3:
=====

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

**Related commands** [show trigger](#)



# undebbug atmf

**Overview** This command is an alias for the **no** variant of the [debug atmf](#) command.

## username (atmf-guest)

**Overview** This command enables you to assign a **username** to a guest class. Guests may require a username and possibly also a password. The password must be between 1 and 32 characters and will allow spaces.

**Syntax** username <name> password [8] <userpass>  
no username

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                 |
|------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <name>     | User name of the guest node.                                                                                                                                                                                                                                                                                                                |
| 8          | The parameter <b>8</b> means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form. |
| <userpass> | The password to be entered for the guest node.                                                                                                                                                                                                                                                                                              |

**Default** No usernames are configured

**Mode** AMF Guest Configuration

**Example** To assign the user name 'reception' and the password of 'secret' to an AMF guest node that has the guest class of 'phone1' use the following commands:

```
node1# configure terminal
node1(config)# amf guest-class phone1
node1(config-atmf-guest)# username reception password secret
```

To remove a guest node username and password for the user guest class 'phone1', use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class phone1
node1(config-atmf-guest)# no username
```

**Related commands** [show atmf links detail](#)  
[atmf guest-class](#)  
[switchport atmf-guestlink](#)  
[show atmf links guest](#)  
[show atmf nodes](#)

# 43

# STOAT Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure Device Discovery using STOAT (Standardized Topology Organizer and Transport).

Using LLDP and DHCP Snooping, STOAT can discover and gather information about devices in the local network. These devices may include IP cameras, IP phones, PCs, laptops, Wi-fi access points, printers, and so on.

Vista Manager EX merges the data from STOAT and existing discovery methods such as AMF, and AMF Plus Device Discovery, to provide a single, accurate and more complete view of the network.

For more information, see the [Device Discovery using STOAT Feature Overview and Configuration Guide](#).

- Command List**
- [“clear stoat collector session counters”](#) on page 2129
  - [“description \(stoat-dest\)”](#) on page 2130
  - [“key \(stoat-dest\)”](#) on page 2131
  - [“name-check \(stoat-dest\)”](#) on page 2132
  - [“service stoat”](#) on page 2133
  - [“show stoat collector”](#) on page 2134
  - [“show stoat destinations”](#) on page 2136
  - [“shutdown \(stoat-dest\)”](#) on page 2138
  - [“stoat collector enable”](#) on page 2139
  - [“stoat collector expiry-period”](#) on page 2140
  - [“stoat collector key”](#) on page 2141
  - [“stoat collector trustpoint”](#) on page 2143
  - [“stoat destination”](#) on page 2144
  - [“trustpoint \(stoat-dest\)”](#) on page 2146

- [“unique-id”](#) on page 2147

# clear stoat collector session counters

**Overview** Use this command to clear the STOAT transport session counters.

**Syntax** `clear stoat collector session counters [<1-4294967295>]`

| Parameter      | Description |
|----------------|-------------|
| <1-4294967295> | Session ID  |

**Mode** Privileged Exec

**Example** To clear all STOAT transport session counters, use the command:

```
awplus# clear stoat collector session counters
```

To clear a specific STOAT transport session counter, use the command:

```
awplus# clear stoat collector session counters 234234234
```

**Related commands**

- [stoat collector trustpoint](#)
- [show stoat collector](#)
- [stoat collector expiry-period](#)
- [stoat collector key](#)

**Command changes** Version 5.5.3-1.1: command added

## description (stoat-dest)

**Overview** Use this command to add an informative description to a STOAT destination.

Use the **no** variant of this command to remove a description from a STOAT destination.

**Syntax** `description <description>`  
`no description`

| Parameter                        | Description                                                                                                                                                                 |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;description&gt;</code> | A word or phrase that uniquely identifies this STOAT destination or its purpose. Valid characters are any printable character and spaces, up to a maximum of 40 characters. |

**Default** Not set.

**Mode** STOAT Destination Configuration

**Example** To add the description 'chc-collector-1' to a STOAT destination with IP address 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# description chc-collector-1
```

To remove the description from a STOAT destination with IP address 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no description
```

**Related commands** [stoat destination](#)

**Command changes** Version 5.5.3-1.1: command added

# key (stoat-dest)

**Overview** Use this command to configure a key to use with a STOAT destination. The key allows the STOAT collector to authenticate this device as a valid source. The destination will not attempt to connect if no key is set.

A matching key must be configured on the STOAT collector device.

Use the **no** variant of this command to remove a key for a STOAT destination.

**Syntax** `key [8] <key-string>`  
`no key`

| Parameter    | Description                                                                                                                                                                                                                                      |
|--------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8            | Specifies that you are entering a password as a string that has already been encrypted instead of entering a plain text password. The running config displays the new password as an encrypted string even if password encryption is turned off. |
| <key-string> | Shared key string applied, a value in the range 8 to 80 characters.                                                                                                                                                                              |

**Default** Not set.

**Mode** STOAT Destination Configuration

**Example** To configure the key 'verysecret' for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# key verysecret
```

To remove the key for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no key
```

**Related commands** [stoat collector key](#)  
[stoat destination](#)

**Command changes** Version 5.5.3-1.1: command added

## name-check (stoat-dest)

**Overview** Use this command to enable or disable certificate name checking for the server certificate received from the STOAT collector.

Use the **no** variant of this command to disable name checking for the server certificate received from the STOAT collector.

**Syntax** name-check  
no name-check

**Default** Disabled.

**Mode** STOAT Destination Configuration

**Usage notes** If enabled, the received server certificate must contain the address configured for this STOAT destination . This setting only takes effect if the STOAT destination has been configured with a trustpoint.

**Example** To enable name-check for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-destination)# name-check
```

To disable name-check for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-destination)# no name-check
```

**Related commands** [service stoat](#)

**Command changes** Version 5.5.3-1.1: command added



# service stoat

**Overview** Use this command to enable or disable Standardized Topology Organizer and Transport (STOAT) functionality on a device. Once enabled, the device will accept STOAT collector and STOAT source configuration.

Use the **no** variant of this command to disable STOAT functionality on a device.

**Syntax** `service stoat`  
`no service stoat`

**Default** Disabled.

**Mode** Global Configuration

**Example** To enable STOAT functionality on a device, use the commands:

```
awplus# configure terminal
awplus(config)# service stoat
```

To disable STOAT functionality on a device, use the commands:

```
awplus# configure terminal
awplus(config)# no service stoat
```

**Related commands** [stoat collector trustpoint](#)  
[stoat collector expiry-period](#)  
[stoat collector key](#)  
[show stoat collector](#)

**Command changes** Version 5.5.3-1.1: command added

# show stoat collector

**Overview** Use this command to see the operational status of the STOAT collector.

**Syntax** `show stoat collector [sessions|keys]`

| Parameter | Description                    |
|-----------|--------------------------------|
| sessions  | Active session information     |
| keys      | Authentication key information |

**Mode** Privileged Exec

**Example** To show the STOAT collector status information, use the command:

```
awplus# show stoat collector
```

To show the STOAT collector active session information, use the command:

```
awplus# show stoat collector sessions
```

To show the STOAT collector authentication key information, use the command:

```
awplus# show stoat collector keys
```

**Output** Figure 43-1: Example output from **show stoat collector**

```
awplus#show stoat collector

STOAT CollectorInformation:

Status : Enabled
Expiry-period : 60 seconds
Trustpoint : default-selfsigned
```

Figure 43-2: Example output from **show stoat collector sessions**

```
awplus#show stoat collector sessions

STOAT Collector Session Information:

Sessions created : 2
Sessions expired : 0
Sessions failed : 0
Sessions failed sync authentication : 0
Sessions failed update : 0
Sessions failed update authentication : 0

Session ID : 3F4B5C27
Source Name : alice
State : Active
Counters
 Update success : 0
 Update authentication failure : 0
 Update failure : 0
 RX payload bytes : 11
 RX payload apteryx set failure : 0
 RX payload json parse failure : 0
 RX payload json decode failure : 0

Session ID : 23DFBD7B
Source Name : bob
State : Active
Counters
 Update success : 0
 Update authentication failure : 0
 Update failure : 0
 RX payload bytes : 0
 RX payload apteryx set failure : 0
 RX payload json parse failure : 0
 RX payload json decode failure : 1
```

Figure 43-3: Example output from **show stoat collector keys**

```
awplus#show stoat collector keys

STOAT Collector Key Information:

Key Description Last Used Time
 (H:M:S ago)

CoA4E6riSbdWzzetHhHM5F5WdBFPXX2DH6jNzZmYtns= "generated key" 00:12:52
secret-key "super secret key" -
```

**Related commands**

- [service stoat](#)
- [stoat collector expiry-period](#)
- [stoat collector enable](#)

**Command changes**

- Version 5.5.3-1.1: command added

# show stoat destinations

**Overview** Use this command to see the operational status of the configured STOAT destinations.

**Syntax** `show stoat destinations [detail]`

| Parameter | Description               |
|-----------|---------------------------|
| detail    | Show detailed information |

**Mode** Privileged Exec

**Example** To show summary information about STOAT destinations, use the command:

```
awplus# show stoat destinations
```

To show detailed information about STOAT destinations, use the command:

```
awplus# show stoat destinations detail
```

**Output** Figure 43-4: Example output from **show stoat destinations**

```
awplus#show stoat destinations
STOAT Destination Summary Information:
-----|
Address : 192.168.0.12
State : Hold

Address : 192.168.0.2
State : Active
```

Figure 43-5: Example output from **show stoat destinations detail**

```
awplus#show stoat destinations detail

STOAT Destination Summary Information:
-----|
Address : 192.168.0.12
State : Hold
Session ID : 0
Expiry-period : 0 seconds
Counters:
 Sync OK : 0
 Sync failed - unreachable : 6612
 Sync failed - authentication : 0
 Sync failed - bad response : 0
 Update OK : 0
 Update failed - unreachable : 0
 Update failed - authentication : 0
 Update failed - unknown session : 0
 RX bytes : 0
 TX bytes : 0
Address : 192.168.0.2
State : Active
Session ID : 200558F4
Expiry-period : 60 seconds
Counters:
 Sync OK : 139
 Sync failed - unreachable : 10
 Sync failed - authentication : 0
 Sync failed - bad response : 0
 Update OK : 32773
 Update failed - unreachable : 52
 Update failed - authentication : 0
 Update failed - unknown session : 81
 RX bytes : 4099
 TX bytes : 16787801
```

**Related commands**   [stoat destination shutdown \(stoat-dest\)](#)

**Command changes**   Version 5.5.3-1.1: command added

# shutdown (stoat-dest)

**Overview** Use this command to disable a STOAT destination.  
Use the **no** variant of this command to enable a STOAT destination.

**Syntax** shutdown  
no shutdown

**Default** Enabled (no shutdown)

**Mode** STOAT Destination Configuration

**Example** To enable the STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no shutdown
```

**Related commands** [stoat destination](#)  
[show stoat destinations](#)

**Command changes** Version 5.5.3-1.1: command added

# stoat collector enable

**Overview** Use this command to start or stop the Standardized Topology Organizer and Transport (STOAT) collector functionality on a device.

Note: The device must be able to receive requests from STOAT sources before this command is used. To enable a device to receive requests from STOAT, use the [service stoat](#) command.

Use the **no** variant of this command to stop the STOAT collector functionality on a device.

**Syntax** `stoat collector enable`  
`no stoat collector enable`

**Default** Disabled.

**Mode** Global Configuration

**Usage notes** The STOAT feature is responsible for discovering devices and network topology, organizing that information into a standardized format, and transporting it to a central location for use. AMF uses STOAT data to allow non-AMF devices and their links to be displayed in the AMF topology map.

There are two types of STOAT device:

- **Collector** - receives and aggregates topology data
- **Source** - sends data to a collector. The data contains information that it knows about itself and has learned through discovery protocols

**Example** To start the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector enable
```

To stop the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector enable
```

**Related commands** [stoat collector trustpoint](#)  
[show stoat collector](#)  
[stoat collector expiry-period](#)  
[stoat collector key](#)

**Command changes** Version 5.5.3-1.1: command added.

# stoat collector expiry-period

**Overview** Use this command to modify the session expiry-period for all of the STOAT collector's sessions.

Use the **no** variant of this command to revert to the default expiry-period of 60 seconds.

**Syntax** `stoat collector expiry-period <10-300>`  
`no stoat collector expiry-period`

| Parameter | Description                            |
|-----------|----------------------------------------|
| <10-300>  | Expiry-period in seconds (default: 60) |

**Default** 60 seconds.

**Mode** Global Configuration

**Example** To configure an expiry-period of 15 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector expiry-period 15
```

To revert the expiry-period to its default of 60 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector expiry-period
```

**Related commands** [service stoat](#)  
[stoat collector trustpoint](#)  
[stoat collector key](#)  
[stoat collector enable](#)  
[show stoat collector](#)

**Command changes** Version 5.5.3-1.1: command added



# stoat collector key

**Overview** Use this command to configure the authentication key used by the STOAT collector.

Use the **no** variant of this command to remove a STOAT authentication key.

**Syntax** `stoat collector key [8]{auth-key|generate} [description <description>]`  
`no stoat collector key [8]{auth-key|generate} [description <description>]`

| Parameter     | Description                                                |
|---------------|------------------------------------------------------------|
| 8             | Specifies a key in encrypted format instead of plain text. |
| auth-key      | Authentication key                                         |
| generate      | Let STOAT generate a key                                   |
| description   | Add a useful description                                   |
| <description> | The useful description text                                |

**Default** Not set.

**Mode** Global Configuration

**Example** To configure a plain-text key 'secret-key' with no description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key secret-key
```

To configure a plain-text key 'secret-key' with a description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key secret-key description
'this is my secret key'
```

To **generate** a key with a description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key generate description 'my
generated key'
```

To configure an encrypted key with a description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key 8
CFWzNguaqyoPDqYoCBGzff07CfQZ0J-eJ00JslXON3E= description 'my
encrypted key'
```

To remove a configured encrypted key, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector key 8
CFWzNguaqyoPDqYoCBGzff07CfQZOJ-eJO0JslXON3E=
```

**Output** Figure 43-6: Example output from **stoat collector key generate**

```
awplus(config)# stoat collector key generate
NttWCIS0KsyQ1-1_98qi4HcVdMRykeaE8IKfPe1Xv9o
```

**Related  
commands**

[service stoat](#)  
[stoat collector trustpoint](#)  
[stoat collector expiry-period](#)  
[stoat collector enable](#)  
[show stoat collector](#)

**Command  
changes**

Version 5.5.3-1.1: command added

# stoat collector trustpoint

**Overview** Use this command to add a crypto PKI trustpoint containing a server certificate and a key to the STOAT collector. This enables secure HTTPS API communication between the STOAT collector and STOAT source.

Use the **no** variant of this command to remove a configured PKI trustpoint from a STOAT collector.

**Syntax** `stoat collector trustpoint <trustpoint-name>`  
`no stoat collector trustpoint`

| Parameter                            | Description          |
|--------------------------------------|----------------------|
| <code>&lt;trustpoint-name&gt;</code> | PKI trustpoint name. |

**Mode** Global Configuration

**Example** To add an existing PKI trustpoint called 'chc' to the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector trustpoint chc
```

To remove a configured PKI trustpoint from the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector trustpoint
```

**Related commands** [crypto pki authenticate](#)  
[crypto pki enroll](#)  
[crypto pki trustpoint](#)

**Command changes** Version 5.5.3-1.1: command added

# stoat destination

**Overview** Use this command to configure a remote STOAT collector destination.  
Use the **no** variant of this command to remove a STOAT collector destination.

**Syntax** `stoat destination {<ip-address>|<host-name>|<ipv6-address>}`  
`no stoat destination {<ip-address>|<host-name>|<ipv6-address>}`

| Parameter                         | Description                                                                                          |
|-----------------------------------|------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code>   | The IPv4 address, using the format A.B.C.D.                                                          |
| <code>&lt;host-name&gt;</code>    | The host name specified in FQDN (Fully Qualified Domain Name). For example, manager.your.domain.com. |
| <code>&lt;ipv6-address&gt;</code> | The IPv6 address, using the format X:X::X:X.                                                         |

**Default** Not set.

**Mode** Global Configuration

**Example** To configure a remote STOAT collector at IP address 10.0.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 10.0.0.1
```

To remove a remote STOAT collector at IP address 10.0.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat destination 10.0.0.1
```

To configure a remote STOAT collector at stoat.com, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination stoat.com
```

To remove a remote STOAT collector at stoat.com, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat destination stoat.com
```

To configure a remote STOAT collector at 2001:db8::1, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 2001:db8::1
```

To remove a remote STOAT collector at 2001:db8::1, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat destination 2001:db8::1
```

**Related commands** [stoat collector key](#)

`show stoat collector`

**Command changes** Version 5.5.3-1.1: command added

# trustpoint (stoat-dest)

**Overview** Use this command to specify the trustpoint to use when authenticating the STOAT collector. If no trustpoint is specified, the STOAT collector will be implicitly trusted without authentication.

Use the **no** variant of this command to stop the use of trustpoints with a specified STOAT destination.

**Syntax** `trustpoint <trustpoint-name>`  
`no trustpoint`

| Parameter                            | Description             |
|--------------------------------------|-------------------------|
| <code>&lt;trustpoint-name&gt;</code> | Name of the trustpoint. |

**Default** Not set.

**Mode** STOAT Destination Configuration

**Example** To configure the STOAT destination 192.0.2.6 to use trustpoint 'chc', use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# trustpoint chc
```

To stop the use of trustpoints with STOAT destination 192.0.2.6 use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no trustpoint
```

**Related commands** [stoat collector trustpoint](#)  
[stoat destination](#)  
[name-check \(stoat-dest\)](#)

**Command changes** Version 5.5.3-1.1: command added

# unique-id

**Overview** Use this command to generate a new unique ID for a device. This ID is used to uniquely identify a device in the STOAT topology.

Some circumstances may require you to generate a new unique ID, for example after recovering a device from an AMF provisioned backup.

**Syntax** `unique-id`

**Mode** Privileged Exec

**Example** To generate a new unique ID for a STOAT device, use the command:

```
awplus# unique-id
```

**Related commands** [service stoat](#)

**Command changes** Version 5.5.3-1.1: command added

# 44

# Device Discovery using SNMP Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure Device Discovery using SNMP.

SNMP Device Discovery is available from the AlliedWare Plus CLI and is also available from Vista Manager mini. This feature provides information that allows the CLI to display third party vendor device data in real time.

For more information, see the [Device Discovery and Monitoring using SNMP Feature Overview and Configuration Guide](#).

- Command List**
- [“clear snmp-discovery”](#) on page 2149
  - [“service snmp-discovery”](#) on page 2150
  - [“show running-config snmp-discovery”](#) on page 2151
  - [“show snmp-discovery”](#) on page 2152
  - [“snmp-discovery arp-polling-interval”](#) on page 2154
  - [“snmp-discovery community”](#) on page 2155
  - [“snmp-discovery deny”](#) on page 2156
  - [“snmp-discovery permit”](#) on page 2158
  - [“snmp-discovery snmp-polling-interval”](#) on page 2159
  - [“snmp-discovery snmp-version”](#) on page 2160
  - [“snmp-discovery user”](#) on page 2161



# clear snmp-discovery

**Overview** Use this command to remove information learned by the SNMP Discovery process.

**Syntax** `clear snmp-discovery ip [<ipv4-address>]`  
`clear snmp-discovery nodes [<ipv4-address>]`

| Parameter      | Description                                                             |
|----------------|-------------------------------------------------------------------------|
| ip             | Internet Protocol (IP)                                                  |
| <ipv4-address> | IPv4 network address for the discovered device, for example 192.168.3.1 |
| nodes          | Node information                                                        |
| <ipv4-address> | IPv4 network address for the discovered nodes, for example 192.168.3.1  |

**Default** No information is cleared.

**Mode** Privileged Exec

**Examples** To remove all SNMP discovered devices, use the command:

```
node1# clear snmp-discovery nodes
```

To remove a particular SNMP discovered device, use the command:

```
node1# clear snmp-discovery nodes 192.168.3.1
```

To remove all entries from SNMP Discovery's database of devices discovered by ARP, use the command:

```
node1# clear snmp-discovery ip
```

To remove a particular entry from SNMP Discovery's database of devices discovered by ARP, use the command:

```
node1# clear snmp-discovery ip 192.168.3.1
```

**Related commands** [show snmp-discovery](#)

**Command changes** Version 5.5.0-0.3: command added

# service snmp-discovery

**Overview** Use this command to enable SNMP Discovery to discover devices on an AMF network.

Use the **no** variant of this command to disable SNMP Discovery.

**Syntax** `service snmp-discovery`  
`no service snmp-discovery`

**Default** Disabled

**Mode** Global Configuration

**Usage notes** The server starts a process which detects IP addresses reachable on a network. An SNMP 'get' request is performed on these IP addresses to detect device information. The SNMP name, SNMP description, SNMP location, and SNMP serial number are obtained if they are available.

SNMP Discovery will not run if there are no Layer 3 IP interfaces configured.

**Example** To start the discovery service on the AMF node, use the commands:

```
awplus# configure terminal
awplus(config)# service snmp-discovery
```

**Related commands** [show snmp-discovery](#)  
[snmp-discovery arp-polling-interval](#)  
[snmp-discovery community](#)  
[snmp-discovery deny](#)  
[snmp-discovery permit](#)  
[snmp-discovery snmp-polling-interval](#)  
[snmp-discovery user](#)  
[snmp-discovery snmp-version](#)

**Command changes** Version 5.5.0-0.3: command added

# show running-config snmp-discovery

**Overview** Use this command to display the running configuration for SNMP Discovery.

**Syntax** `show running-config snmp-discovery`

**Mode** Privileged Exec

**Example** To display the running configuration for SNMP Discovery, use the command:

```
awplus# show running-config snmp-discovery
```

**Output** Figure 44-1: Example output from **show running-config snmp-discovery**

```
node1#show running-config snmp-discovery
service snmp-discovery
snmp-discovery community accounting
snmp-discovery user tim encrypted auth md5
U2FsdGVkX1/LyNttTLDzgJjTG6Eh5g2L4ahgXuHLENA= priv des
U2FsdGVkX1+FJsefN+ZvSzUUviRt9ZdsFwtB6HU12lU=
snmp-discovery permit ip 192.168.3.2
snmp-discovery permit ip 192.168.3.6
snmp-discovery deny ip 192.168.3.5
```

**Related commands** [show snmp-discovery](#)

**Command changes** Version 5.5.0-0.3: command added

# show snmp-discovery

**Overview** Use this command to show information about the SNMP Discovery process.

**Syntax** `show snmp-discovery [detail|ip|nodes]`

| Parameter | Description                     |
|-----------|---------------------------------|
| detail    | SNMP Discovery node detail      |
| ip        | SNMP Discovery IP addresses     |
| nodes     | SNMP Discovery node information |

**Mode** User Exec

**Examples** To display information about the SNMP Discovery status, use the command:

```
awplus# show snmp-discovery
```

To display information about the SNMP Discovery IPv4 addresses learned, use the command:

```
awplus# show snmp-discovery ip
```

To display information about the SNMP Discovery nodes learned, use the command:

```
awplus# show snmp-discovery nodes
```

To display information about the SNMP Discovery in greater detail, use the command:

```
awplus# show snmp-discovery detail
```

**Output** Figure 44-2: Example output from **show snmp-discovery**

```
awplus#show snmp-discovery

SNMP Discovery information:

SNMP Discovery : Enabled
SNMP Polling interval : 300
ARP Polling interval : 60
SNMP Discovery version : v2c
SNMPv2 Discovery Community : accounting
```

Figure 44-3: Example output from **show snmp-discovery ip**

```
node1#show snmp-discovery ip
SNMP Discovery Devices:
```

| IP Address     | MAC Address    | Type    | State       | Last Seen Time        |
|----------------|----------------|---------|-------------|-----------------------|
| 172.18.100.10  | -              | Permit  | -           | -                     |
| 172.18.100.25  | 0000.cd28.063e | Dynamic | Up          | -                     |
| 172.18.100.15  | 0001.30fe.c080 | Dynamic | Up          | -                     |
| 172.18.100.208 | 801f.0230.006c | Dynamic | Down        | Jul 27, 2020 03:52:01 |
| 172.18.100.209 | 801f.0230.006c | Dynamic | Down        | Jul 24, 2020 04:45:30 |
| 172.18.100.20  | 0010.db5c.efef | Dynamic | Up          | -                     |
| 172.18.100.207 | 801f.0230.006c | Dynamic | Down        | Jul 27, 2020 06:26:20 |
| 172.18.100.10  | 001b.5443.a5b0 | Dynamic | Up          | -                     |
| 172.18.100.205 | 801f.0230.006c | Dynamic | Down        | Jul 27, 2020 17:15:15 |
| 172.18.100.204 | 801f.0230.006c | Dynamic | Down        | Jul 25, 2020 19:20:35 |
| 172.18.100.203 | 801f.0230.006c | Dynamic | Down        | Jul 25, 2020 21:15:04 |
| 172.18.100.202 | 801f.0230.006c | Dynamic | Unreachable | Jul 28, 2020 10:20:10 |

Figure 44-4: Example output from **show snmp-discovery nodes**

```
node1#show snmp-discovery nodes
SNMP Discovery Node information:
```

| System Name     | IP Address    | MAC Address    | Description                  |
|-----------------|---------------|----------------|------------------------------|
| TQ1402          | 172.18.100.15 | 0001.30fe.c080 | wireless access point ...    |
| NAT-ROUTER-DESK | 172.18.100.25 | 0000.cd28.063e | CentreCOM AR570S version ... |

Number of SNMP discovered nodes: 2

**Related commands**

- [clear snmp-discovery](#)
- [service snmp-discovery](#)
- [show running-config snmp-discovery](#)
- [snmp-discovery arp-polling-interval](#)
- [snmp-discovery deny](#)
- [snmp-discovery permit](#)
- [snmp-discovery snmp-polling-interval](#)

**Command changes** Version 5.5.0-0.3: command added

# snmp-discovery arp-polling-interval

**Overview** Use this command to configure the SNMP ARP polling interval.

Use the **no** variant of this command to set the SNMP ARP polling interval back to the default (60 seconds).

**Syntax** `snmp-discovery arp-polling-interval <1-3600>`  
`no snmp-discovery arp-polling-interval`

| Parameter | Description                                                            |
|-----------|------------------------------------------------------------------------|
| <1-3600>  | The polling number in seconds to interval in the range from 1 to 3600. |

**Default** ARP requests are sent out every 60 seconds

**Mode** Global Configuration

**Usage notes** SNMP Discovery first uses ARP to discover subnets that are reachable from the AMF node. This polling happens every 60 seconds by default. Use this command to change the polling interval.

**Examples** To configure the SNMP Discovery ARP polling interval to 120 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-discovery arp-polling-interval 120
```

To set the SNMP Discovery ARP polling interval back to the default (60 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-discovery arp-polling-interval
```

**Related commands** [service snmp-discovery](#)  
[show snmp-discovery](#)

**Command changes** Version 5.5.0-0.3: command added

# snmp-discovery community

**Overview** Use this command to create an SNMP community in read-only mode for SNMPv1 and v2c only.

Use the **no** variant of this command to remove an SNMP community.

**Syntax** `snmp-discovery community <community-name>`

| Parameter                           | Description                                                                           |
|-------------------------------------|---------------------------------------------------------------------------------------|
| <code>&lt;community-name&gt;</code> | The name of the community that can be up to 20 characters long and is case sensitive. |

**Default** The SNMP Discovery community name is 'public' by default

**Mode** Global Configuration

**Usage notes** This command creates an SNMP community in read-only mode. The community allows access to all MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used for SNMPv3.

**Examples** To configure an SNMP community named 'accounting', use the commands:

```
awplus# configure terminal
awplus(config)# snmp-discovery community accounting
```

To set the SNMP community name back to the default (public), use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-discovery community
```

**Related commands** [service snmp-discovery](#)  
[show snmp-discovery](#)

**Command changes** Version 5.5.0-0.3: command added

# snmp-discovery deny

**Overview** Use this command to prevent ARP requests from being sent. When an interface or IPv4 address is denied, it means an ARP request and SNMP 'get' request will never be sent to that device when the command **service snmp-discovery** is enabled.

Use the **no** variant of this command to remove the configuration.

**Syntax**

```
snmp-discovery deny interface <interface-range>
snmp-discovery deny ip <ipv4-address>
no snmp-discovery deny interface <interface-range>
no snmp-discovery deny ip <ipv4-address>
```

| Parameter        | Description                      |
|------------------|----------------------------------|
| interface        | Interfaces to deny               |
| <interface-name> | Interface name, for example eth1 |
| ip               | IP address                       |
| <ipv4-address>   | IPv4 address to deny             |

**Default** The AMF management VLAN is denied

**Mode** Global Configuration

**Examples** To configure a deny interface command for eth1, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-discovery deny interface eth1
```

To stop interface eth1 from being denied, use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-discovery deny interface eth1
```

To configure a deny IP command for IP address 192.168.3.2, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-discovery deny ip 192.168.3.2
```

To stop IP address 192.168.3.2 from being denied, use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-discovery deny ip 192.168.3.2
```



**Output** Figure 44-5: Example output from **show snmp-discovery ip**

```
awplus#show snmp-discovery ip
SNMP Discovery Devices:
```

| IP Address  | MAC Address    | Type    | State | Last Seen Time        |
|-------------|----------------|---------|-------|-----------------------|
| -----       |                |         |       |                       |
| 192.168.3.2 | -              | Deny    | -     | -                     |
| 1.2.3.6     | -              | Permit  | -     | 30 Jul, 2020 06:30:55 |
| 1.2.3.4     | -              | Permit  | -     | 31 Jul, 2020 05:49:04 |
| 192.168.2.2 | 3863.bb5c.b900 | Dynamic | Up    | -                     |

**Related commands** [service snmp-discovery](#)  
[show snmp-discovery](#)

**Command changes** Version 5.5.0-0.3: command added

# snmp-discovery permit

**Overview** Use this command if you want to allow SNMP Discovery to do requests on interfaces with greater than 256 members. You can permit a specific IP address.

**Syntax** `snmp-discovery permit ip <ipv4-address>`  
`no snmp-discovery permit ip <ipv4-address>`

| Parameter      | Description            |
|----------------|------------------------|
| ip             | Internet Protocol (IP) |
| <ipv4-address> | IPv4 network address   |

**Default** All IPv4 interfaces with 256 members or less are included in SNMP Discovery.

**Mode** Global Configuration

**Examples** To configure a permit IP command for the address 192.168.3.2, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# snmp-discovery permit ip 192.168.3.2
```

To remove the permit configuration for the address 192.168.3.2, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no snmp-discovery permit ip 192.168.3.2
```

**Output** Figure 44-6: Example output from **show snmp-discovery ip**

```
awplus#show snmp-discovery ip
SNMP Discovery Devices:
```

| IP Address  | MAC Address    | Type    | State | Last Seen Time        |
|-------------|----------------|---------|-------|-----------------------|
| 1.2.3.5     | -              | Deny    | -     | -                     |
| 1.2.3.6     | -              | Permit  | -     | Jul 27, 2020 03:33:39 |
| 1.2.3.4     | -              | Permit  | -     | Jul 28, 2020 04:25:05 |
| 192.168.2.2 | 3863.bb5c.b900 | Dynamic | Up    | -                     |
| 192.168.3.2 | 4263.cc3c.b500 | permit  | Up    | -                     |

**Related commands** [service snmp-discovery](#)  
[show snmp-discovery](#)

**Command changes** Version 5.5.0-0.3: command added

# snmp-discovery snmp-polling-interval

**Overview** Use this command to change the SNMP request polling interval (in seconds).  
Use the **no** variant of this command to set the SNMP request polling interval back to the default (300 seconds).

**Syntax** `snmp-discovery snmp-polling-interval <60-3600>`  
`no snmp-discovery snmp-polling-interval`

| Parameter | Description                                                                     |
|-----------|---------------------------------------------------------------------------------|
| <60-3600> | The number of seconds for the SNMP polling interval. From the range 60 to 3600. |

**Default** 300 seconds (5 minutes)

**Mode** Global Configuration

**Usage notes** ARP polling and SNMP Discovery uses SNMP 'get' requests to poll the devices discovered by the ARP polling. This polling happens every 300 seconds (5 minutes) by default.

SNMP polling is enabled when **service snmp-discovery** is enabled.

**Examples** To configure the SNMP discovery polling interval to 120 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-discovery snmp-polling-interval 120
```

To set the SNMP discovery polling interval back to the default (300 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-discovery snmp-polling-interval
```

**Related commands** [service snmp-discovery](#)  
[show snmp-discovery](#)

**Command changes** Version 5.5.0-0.3: command added

# snmp-discovery snmp-version

**Overview** Use this command to set the SNMP version that you are using.

Use the **no** variant of this command to set the SNMP version back to the default (v2c).

**Syntax** `snmp-discovery snmp-version {v1|v2c|v3}`  
`no snmp-discovery snmp-version`

| Parameter | Description                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------|
| v1        | Enter the SNMP version number you are using                                                                |
| v2c       | If you are using SNMP version v2c, set the community name with the command <b>snmp-discovery community</b> |
| v3        | If you are using SNMP version v3, set the security with the command <b>snmp-discovery user</b>             |

**Default** SNMP version v2c

**Mode** Global Configuration

**Usage notes** This command defaults to SNMP version v2c and creates an SNMP community in read-only mode. The community allows access to all the MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used when operating SNMPv3.

If using SNMPv3, you can choose the security level and then the authentication protocol and privacy protocol.

**Examples** To configure SNMP Discovery to use SNMP version 3, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-discovery snmp-version v3
```

To set the SNMP Discovery SNMP version back to the default (v2c), use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-discovery snmp-version
```

**Related commands** [service snmp-discovery](#)

**Command changes** Version 5.5.0-0.3: command added

# snmp-discovery user

**Overview** Use this command to create a user for SNMPv3 'get' requests only.

Use the **no** variant of this command to remove an SNMPv3 user.

**Syntax** `snmp-discovery user <user-name> [encrypted] [auth {md5|sha} <auth-password>] [priv {des|aes} <privacy-password>]`  
`no snmp-discovery user <user-name>`

| Parameter          | Description                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------|
| <user-name>        | The user name is a string up to 20 characters long and is case sensitive. For example, 'Rodger'. |
| encrypted          | Use the encrypted parameter when you want to enter encrypted passwords.                          |
| auth               | Authentication protocol that can be either MD5 or SHA.                                           |
| md5                | MD5 Message Digest Algorithms.                                                                   |
| sha                | SHA Secure Hash Algorithm.                                                                       |
| <auth-password>    | Authentication password that is a string from 8 to 20 characters and is case sensitive.          |
| priv               | Privacy protocol that can be either DES or AES.                                                  |
| des                | DES Data Encryption Standard.                                                                    |
| aes                | AES Advanced Encryption Standards.                                                               |
| <privacy-password> | Privacy password is a string from 8 to 20 characters and is case sensitive.                      |

**Default** No user is configured

**Mode** Global Configuration

**Usage notes** Additionally, this command provides the option of selecting an authentication protocol and (where appropriate) an associated password. Similarly, options are offered for selecting a privacy protocol and password.

The authentication method must match what is used on the devices being configured.

Use the **encrypted** parameter when you want to enter already encrypted passwords in encrypted form as displayed in the running and startup configurations stored on the switch.

User passwords are entered using plain text without the **encrypted** parameter and are encrypted according to the authentication and privacy protocols selected.

User passwords are viewed as encrypted passwords in running and startup configurations shown from the **show running-config** and **show startup-config**

commands. Copy and paste encrypted passwords from the running configuration or startup configuration to avoid entry errors.

**Examples** To add SNMP Discovery user 'authuser' with authentication protocol 'md5', authentication password 'authpass' privacy protocol 'des' and privacy password privpass, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-discovery user authuser auth md5 Authpass
priv des Privpass
```

To enter existing SNMP user 'authuser' with existing passwords with authentication protocol 'md5' plus the encrypted authentication password '0x1c74b9c22118291b0ce0cd883f8dab6b74', privacy protocol 'des' plus the encrypted privacy password '0x0e0133db5453ebd03822b004eeacb6608f', use the following commands:

*Note Copy and paste the encrypted passwords from the running-config or the startup-config displayed, using the show running-config and show startup-config commands respectively, into the command line to avoid key stroke errors issuing this command.*

```
awplus# configure terminal
awplus(config)# snmp-discovery user authuser encrypted auth
md50x1c74b9c22118291b0ce0cd883f8dab6b74 priv des
0x0e0133db5453ebd03822b004eeacb6608f
```

To delete SNMP user 'authuser', use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-discovery user authuser
```

**Output** Figure 44-7: Example output from **show snmp-discovery**

```
awplus#show snmp-discovery
SNMP Discovery information:

SNMP Discovery : Enabled
SNMP Polling interval : 300
ARP Polling interval : 60
SNMP Discovery version : v3

SNMPv2 Discovery Community : accounting
SNMPv3 Discovery User : authuser
User Encrypted auth : md5
User Encrypted password : 0x1c74b9c22118291b0ce0cd883f8dab6b74
User Privilege : des
User Privilege password : 0x0e0133db5453ebd03822b004eeacb6608f
```

**Related commands** [service snmp-discovery](#)  
[show snmp-discovery](#)

**Command changes** Version 5.5.0-0.3: command added

# 45

# Dynamic Host Configuration Protocol (DHCP) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure DHCP.

Note that the DHCP client does not support tunnel interfaces.

For more information, see the [DHCP Feature Overview and Configuration Guide](#).

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Command List**
- [“bootfile”](#) on page 2165
  - [“clear ip dhcp binding”](#) on page 2166
  - [“default-router”](#) on page 2167
  - [“dns-server”](#) on page 2168
  - [“domain-name”](#) on page 2169
  - [“host \(DHCP\)”](#) on page 2170
  - [“ip address dhcp”](#) on page 2171
  - [“ip dhcp bootp ignore”](#) on page 2173
  - [“ip dhcp leasequery enable”](#) on page 2174
  - [“ip dhcp option”](#) on page 2175
  - [“ip dhcp pool”](#) on page 2177
  - [“ip dhcp-client default-route distance”](#) on page 2178
  - [“ip dhcp-client request vendor-identifying-specific”](#) on page 2180
  - [“ip dhcp-client vendor-identifying-class”](#) on page 2181
  - [“ip dhcp-relay agent-option”](#) on page 2182
  - [“ip dhcp-relay agent-option checking”](#) on page 2184

- ["ip dhcp-relay agent-option remote-id"](#) on page 2185
- ["ip dhcp-relay information policy"](#) on page 2186
- ["ip dhcp-relay maxhops"](#) on page 2188
- ["ip dhcp-relay max-message-length"](#) on page 2189
- ["ip dhcp-relay server-address"](#) on page 2191
- ["ip dhcp-relay short-lease"](#) on page 2193
- ["ip dhcp-relay use-client-side-address"](#) on page 2194
- ["lease"](#) on page 2195
- ["network \(DHCP\)"](#) on page 2197
- ["next-server"](#) on page 2198
- ["option"](#) on page 2199
- ["probe enable"](#) on page 2201
- ["probe packets"](#) on page 2202
- ["probe timeout"](#) on page 2203
- ["probe type"](#) on page 2204
- ["range"](#) on page 2205
- ["route"](#) on page 2206
- ["service dhcp-relay"](#) on page 2207
- ["service dhcp-server"](#) on page 2208
- ["short-lease-threshold"](#) on page 2209
- ["show counter dhcp-client"](#) on page 2211
- ["show counter dhcp-relay"](#) on page 2212
- ["show counter dhcp-server"](#) on page 2215
- ["show dhcp lease"](#) on page 2217
- ["show ip dhcp binding"](#) on page 2218
- ["show ip dhcp pool"](#) on page 2220
- ["show ip dhcp-relay"](#) on page 2225
- ["show ip dhcp server statistics"](#) on page 2226
- ["show ip dhcp server summary"](#) on page 2228
- ["subnet-mask"](#) on page 2229



# bootfile

**Overview** This command sets the boot filename for a DHCP server pool. This is the name of the boot file that the client should use in its bootstrap process. It may need to include a path.

The **no** variant of this command removes the boot filename from a DHCP server pool.

**Syntax** `bootfile <filename>`  
`no bootfile`

| Parameter                     | Description         |
|-------------------------------|---------------------|
| <code>&lt;filename&gt;</code> | The boot file name. |

**Mode** DHCP Configuration

**Example** To configure the boot filename for a pool P2, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# bootfile boot/main_boot.bt
```

# clear ip dhcp binding

**Overview** This command clears either a specific lease binding or the lease bindings specified by the command or DHCP server. The command will only take effect on dynamically allocated bindings, not statically configured bindings.

**Syntax** `clear ip dhcp binding {ip <ip-address>|mac <mac-address>|all|pool <pool-name>|range <low-ip-address> <high-ip-address>}`

| Parameter                                                         | Description                                                                                                                                                                        |
|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ip &lt;ip-address&gt;</code>                                | IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D.                                                                                                 |
| <code>mac &lt;mac-address&gt;</code>                              | MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH.                                                                                              |
| <code>all</code>                                                  | All DHCP bindings.                                                                                                                                                                 |
| <code>pool &lt;pool-name&gt;</code>                               | Description used to identify DHCP server address pool. Valid characters are any printable character. If the name contains spaces then you must enclose these in "quotation marks". |
| <code>range &lt;low-ip-address&gt; &lt;high-ip-address&gt;</code> | IPv4 address range for DHCP clients, in dotted decimal notation. The first IP address is the low end of the range, the second IP address is the high end of the range.             |

**Mode** User Exec and Privileged Exec

**Usage** A specific binding may be deleted by **ip** address or **mac** address, or several bindings may be deleted at once using **all**, **pool** or **range**.

Note that if you specify to clear the **ip** or **mac** address of what is actually a static DHCP binding, an error message is displayed. If **all**, **pool** or **range** are specified and one or more static DHCP bindings exist within those addresses, any dynamic entries within those addresses are cleared but any static entries are not cleared.

**Examples** To clear the specific IP address binding 192.168.1.1, use the command:

```
awplus# clear ip dhcp binding ip 192.168.1.1
```

To clear all dynamic DHCP entries, use the command:

```
awplus# clear ip dhcp binding all
```

**Related commands** [show ip dhcp binding](#)

# default-router

**Overview** This command adds a default router to the DHCP address pool you are configuring. You can use this command multiple times to create a list of default routers on the client's subnet. This sets the router details using the pre-defined option 3. Note that if you add a user-defined option 3 using the **option** command, then you will override any settings created with this command.

The **no** variant of this command removes either the specified default router, or all default routers from the DHCP pool.

**Syntax** `default-router <ip-address>`  
`no default-router [<ip-address>]`

| Parameter                       | Description                                                     |
|---------------------------------|-----------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code> | IPv4 address of the default router, in dotted decimal notation. |

**Mode** DHCP Configuration

**Examples** To add a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# default-router 192.168.1.2
```

To remove a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router 192.168.1.2
```

To remove all routers from the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router
```

# dns-server

**Overview** This command adds a Domain Name System (DNS) server to the DHCP address pool you are configuring. You can use this command multiple times to create a list of DNS name servers available to the client. This sets the DNS server details using the pre-defined option 6.

Note that if you add a user-defined option 6 using the [option](#) command, then you will override any settings created with this command.

The **no** variant of this command removes either the specified DNS server, or all DNS servers from the DHCP pool.

**Syntax** `dns-server <ip-address>`  
`no dns-server [<ip-address>]`

| Parameter                       | Description                                                 |
|---------------------------------|-------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code> | IPv4 address of the DNS server, in dotted decimal notation. |

**Mode** DHCP Configuration

**Examples** To add the DNS server with the assigned IP address 192.168.1.1 to the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# dns-server 192.168.1.1
```

To remove the DNS server with the assigned IP address 192.168.1.1 from the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no dns-server 192.168.1.1
```

To remove all DNS servers from the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no dns-server
```

**Related commands** [default-router](#)  
[option](#)  
[service dhcp-server](#)  
[show ip dhcp pool](#)  
[subnet-mask](#)

# domain-name

**Overview** This command adds a domain name to the DHCP address pool you are configuring. Use this command to specify the domain name that a client should use when resolving host names using the Domain Name System. This sets the domain name details using the pre-defined option 15.

Note that if you add a user-defined option 15 using the [option](#) command, then you will override any settings created with this command.

The **no** variant of this command removes the domain name from the address pool.

**Syntax** `domain-name <domain-name>`  
`no domain-name`

| Parameter                        | Description                                                                                                                                                                |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;domain-name&gt;</code> | The domain name you wish to assign the DHCP pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks". |

**Mode** DHCP Configuration

**Examples** To add the domain name Nerv\_Office to DHCP pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# domain-name Nerv_Office
```

To remove the domain name Nerv\_Office from DHCP pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no domain-name Nerv_Office
```

**Related commands**

- [default-router](#)
- [dns-server](#)
- [option](#)
- [service dhcp-server](#)
- [show ip dhcp pool](#)
- [subnet-mask](#)

# host (DHCP)

**Overview** This command adds a static host address to the DHCP address pool you are configuring. The client with the matching MAC address is permanently assigned this IP address. No other clients can request it.

The **no** variant of this command removes the specified host address from the DHCP pool. Use the **no host all** command to remove all static host addresses from the DHCP pool.

**Syntax** `host <ip-address> <mac-address>`  
`no host <ip-address>`  
`no host all`

| Parameter                        | Description                                                                          |
|----------------------------------|--------------------------------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code>  | IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D    |
| <code>&lt;mac-address&gt;</code> | MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH |

**Mode** DHCP Configuration

**Usage** Note that a network/mask must be configured using a **network** command before issuing a **host** command. Also note that a host address must match a network to add a static host address.

**Examples** To add the host at 192.168.1.5 with the MAC address 000a.451d.6e34 to DHCP pool 1, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool 1
awplus(dhcp-config)# network 192.168.1.0/24
awplus(dhcp-config)# host 192.168.1.5 000a.451d.6e34
```

To remove the host at 192.168.1.5 with the MAC address 000a.451d.6e34 from DHCP pool 1, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool 1
awplus(dhcp-config)# no host 192.168.1.5 000a.451d.6e34
```

**Related  
Commands** [lease](#)  
[range](#)

[show ip dhcp pool](#)

# ip address dhcp

**Overview** This command activates the DHCP client on the interface you are configuring. This allows the interface to use the DHCP client to obtain its IP configuration details from a DHCP server on its connected network.

The **client-id** and **hostname** parameters are identifiers that you may want to set in order to interoperate with your existing DHCP infrastructure. If neither option is needed, then the DHCP server uses the MAC address field of the request to identify the host.

The DHCP client supports the following IP configuration options:

- Option 1— the subnet mask for your device.
- Option 3— a list of default routers.
- Option 6 — a list of DNS servers. This list appends the DNS servers set on your device with the [ip name-server](#) command.
- Option 15—a domain name used to resolve host names. This option replaces the domain name set with the [ip domain-name](#) command. Your device ignores this domain name if it has a domain list set using the [ip domain-list](#) command.
- Option 51—lease expiration time.

The **no** variant of this command stops the interface from obtaining IP configuration details from a DHCP server.

**Syntax** `ip address dhcp [client-id <interface>] [hostname <hostname>]`  
`no ip address dhcp`

| Parameter                                                | Description                                                                                                                                                                                                                            |
|----------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>client-id</code><br><code>&lt;interface&gt;</code> | The name of the interface you are activating the DHCP client on. If you specify this, then the MAC address associated with the specified interface is sent to the DHCP server in the optional identifier field.<br>Default: no default |
| <code>hostname</code><br><code>&lt;hostname&gt;</code>   | The hostname for the DHCP client on this interface. Typically this name is provided by the ISP.<br>Default: no default                                                                                                                 |

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Examples** To set the interface eth0 to use DHCP to obtain an IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip address dhcp
```

To stop the interface eth0 from using DHCP to obtain its IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip address dhcp
```

**Related commands**

- [ip address \(IP Addressing and Protocol\)](#)
- [show ip interface](#)
- [show running-config](#)



# ip dhcp bootp ignore

**Overview** This command configures the DHCP server to ignore any BOOTP requests it receives. The DHCP server accepts BOOTP requests by default.

The **no** variant of this command configures the DHCP server to accept BOOTP requests. This is the default setting.

**Syntax** `ip dhcp bootp ignore`  
`no ip dhcp bootp ignore`

**Mode** Global Configuration

**Examples** To configure the DHCP server to ignore BOOTP requests, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp bootp ignore
```

To configure the DHCP server to respond to BOOTP requests, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp bootp ignore
```

**Related commands** [show ip dhcp server summary](#)

# ip dhcp leasequery enable

**Overview** Use this command to enable the DHCP server to respond to DHCPLEASEQUERY packets. Enabling the DHCP leasequery feature allows a DHCP Relay Agent to obtain IP address information directly from the DHCP server using DHCPLEASEQUERY messages.

Use the **no** variant of this command to disable the support of DHCPLEASEQUERY packets.

For more information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp leasequery enable`  
`no ip dhcp leasequery enable`

**Default** DHCP leasequery support is disabled by default.

**Mode** Global Configuration

**Examples** To enable DHCP leasequery support, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp leasequery enable
```

To disable DHCP leasequery support, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp leasequery enable
```

**Related commands** [show counter dhcp-server](#)  
[show ip dhcp server statistics](#)  
[show ip dhcp server summary](#)

# ip dhcp option

**Overview** This command creates a user-defined DHCP option. Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

You can use this option when configuring a DHCP pool, by using the [option](#) command.

The **no** variant of this command removes either the specified user-defined option, or removes all user-defined options. This also automatically removes the user-defined options from the associated DHCP address pools.

**Syntax** `ip dhcp option <1-254> [name <option-name>] [<option-type>]`  
`no ip dhcp option [<1-254>|<option-name>]`

| Parameter     | Description                                                                                                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-254>       | The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.                                                                                               |
| <option-name> | Option name used to identify the option. You cannot use a number as the option name. Valid characters are any printable character. If the name contains spaces then you must enclose it in “quotation marks”.<br>Default: no default |
| <option-type> | The option value. You must specify a value that is appropriate to the option type:                                                                                                                                                   |
| ascii         | An ASCII text string                                                                                                                                                                                                                 |
| hex           | A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.                                          |
| ip            | An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually by using the option command multiple times.                                        |
| integer       | A number from 0 to 4294967295.                                                                                                                                                                                                       |
| flag          | A value that either sets (to 1) or unsets (to 0) a flag: <b>true</b> , <b>on</b> , or <b>enabled</b> will set the flag. <b>false</b> , <b>off</b> or <b>disabled</b> will unset the flag.                                            |

**Mode** Global Configuration

**Examples** To define a user-defined ASCII string option as option 66, without a name, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp option 66 ascii
```

To define a user-defined hexadecimal string option as option 46, with the name `tcpip-node-type`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp option 46 name tcpip-node-type hex
```

To define a user-defined IP address option as option 175, with the name `special-address`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp option 175 name special-address ip
```

To remove the specific user-defined option with the option number 12, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option 12
```

To remove the specific user-defined option with the option name `perform-router-discovery`, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option perform-router-discovery
```

To remove all user-defined option definitions, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option
```

**Related commands**

[default-router](#)  
[dns-server](#)  
[domain-name](#)  
[option](#)  
[service dhcp-server](#)  
[show ip dhcp server summary](#)  
[subnet-mask](#)

# ip dhcp pool

**Overview** This command will enter the configuration mode for the pool name specified. If the name specified is not associated with an existing pool, the device will create a new pool with this name, then enter the configuration mode for the new pool.

Once you have entered the DHCP configuration mode, all commands executed before the next **exit** command will apply to this pool.

You can create multiple DHCP pools on devices with multiple interfaces. This allows the device to act as a DHCP server on multiple interfaces to distribute different information to clients on the different networks.

The **no** variant of this command deletes the specific DHCP pool.

**Syntax** `ip dhcp pool <pool-name>`  
`no ip dhcp pool <pool-name>`

| Parameter                      | Description                                                                                                                                                           |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;pool-name&gt;</code> | Description used to identify this DHCP pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks". |

**Mode** Global Configuration

**Example** To create the DHCP pool named P2 and enter DHCP Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)#
```

To delete the DHCP pool named P2, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp pool P2
```

**Related commands** [service dhcp-server](#)

# ip dhcp-client default-route distance

**Overview** Use this command to specify an alternative Administrative Distance (AD) for the current default route (from DHCP) for an interface.

Use the **no** variant of this command to set the AD back to the default of 1.

**Syntax** `ip dhcp-client default-route distance [<1-255>]`  
`no ip dhcp-client default-route distance`

| Parameter | Description                                               |
|-----------|-----------------------------------------------------------|
| <1-255>   | Administrative Distance (AD) from the range 1 though 255. |

**Default** 1

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** DHCP client interfaces can automatically add a default route with an AD of 1 into the IP Routing Information Base (RIB).

Any pre-existing default route(s) via alternative interfaces (configured with a higher AD) will no longer be selected as the preferred forwarding path for traffic when the DHCP based default route is added to the IP routing table.

This can be problematic if the DHCP client is operating via an interface that is only intended to be used for back-up interface redundancy purposes.

Use this command to set the AD of the default route (via a specific DHCP client interface) to a non-default (higher cost) value, ensuring any pre-existing default route(s) via any other interface(s) continue to be selected as the preferred forwarding path for network traffic.

When the command is used, the static default route is deleted from the RIB, the distance value of the route is modified to the configured distance value, then it is reinstalled into the RIB.

**Examples** To set the AD for the default route added by DHCP via cellular interface eth0 to 150, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-client default-route distance 150
```

To set the AD for the default route back to the default value of 1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-client default-route distance
```

**Related commands** [show ip route](#)  
[show ip route database](#)

**Command changes** Version 5.4.7-0.2 Command added.

# ip dhcp-client request vendor-identifying-specific

**Overview** Use this command to add vendor-identifying vendor-specific information (option 125) requests to the DHCP discovery packets sent by an interface. This option, along with option 124, can be used to send vendor-specific information back to a DHCP client.

See RFC3925 for more information on Vendor-Identifying Vendor Options for DHCPv4.

Use the **no** variant of this command to remove the vendor-identifying-specific request from an interface.

**Syntax** `ip dhcp-client request vendor-identifying-specific`  
`no ip dhcp-client request vendor-identifying-specific`

**Default** The vendor-identifying-specific request is not configured by default.

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** The DHCP client must be activated on the interface, using the [ip address dhcp](#) command, so that DHCP discovery packets are sent.

**Example** To add the vendor-identifying-specific request on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-client request
vendor-identifying-specific
```

To remove the vendor-identifying-specific request on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-client request
vendor-identifying-specific
```

**Related commands** [ip address dhcp](#)  
[ip dhcp-client vendor-identifying-class](#)

**Command changes** Version 5.4.7-2.1: command added



# ip dhcp-client vendor-identifying-class

**Overview** Use this command to add a vendor-identifying vendor class (option 124) to the DHCP discovery packets sent by an interface. This option places the Allied Telesis Enterprise number (207) into the discovery packet. Option 124, along with option 125, can be used to send vendor-specific information back to a DHCP client.

See RFC3925 for more information on Vendor-Identifying Vendor Options for DHCPv4.

Use the **no** variant of this command to remove the vendor-identifying-class from an interface.

**Syntax** `ip dhcp-client vendor-identifying-class`  
`no ip dhcp-client vendor-identifying-class`

**Default** The vendor-identifying-class is not configured by default.

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** The DHCP client must be activated on the interface, using the [ip address dhcp](#) command, so that DHCP discovery packets are sent.

**Example** To remove the vendor-identifying-class on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-client vendor-identifying-class
```

**Related commands** [ip address dhcp](#)  
[ip dhcp-client request vendor-identifying-specific](#)

**Command changes** Version 5.4.7-2.1: command added

# ip dhcp-relay agent-option

**Overview** This command enables the DHCP Relay Agent to insert the DHCP Relay Agent Information Option (Option 82) into the client-request packets that it relays to its DHCP server. This allows the DHCP Relay Agent to pass on information to the server about the network location of the client device. The DHCP Relay Agent strips the DHCP Relay Agent Option 82 field out of the DHCP server's response, so that the DHCP client never sees this field.

When the DHCP Relay Agent appends its DHCP Relay Agent Option 82 data into the packet, it first overwrites any pad options present; then if necessary, it increases the packet length to accommodate the DHCP Relay Agent Option 82 data.

The **no** variant of this command stops the DHCP Relay Agent from appending the Option 82 field onto DHCP requests before forwarding it to the server.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**NOTE:** The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands [ip dhcp-relay agent-option](#) and [ip dhcp-relay information policy](#) have been configured.

**Syntax** `ip dhcp-relay agent-option`  
`no ip dhcp-relay agent-option`

**Default** DHCP Relay Agent Information Option (Option 82) insertion is disabled by default.

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** Use this command to alter the DHCP Relay Agent Option 82 setting when your device is the first hop for the DHCP client. To limit the maximum length of the packet, use the [ip dhcp-relay max-message-length](#) command.

**Examples** To make the relay agent listening on eth0 append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the relay agent from appending the DHCP Relay Agent Option 82 field on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay agent-option
```

**Related commands**

- [ip dhcp-relay agent-option remote-id](#)
- [ip dhcp-relay information policy](#)
- [ip dhcp-relay max-message-length](#)
- [service dhcp-relay](#)

# ip dhcp-relay agent-option checking

**Overview** This command enables the DHCP Relay Agent to check DHCP Relay Agent Information Option (Option 82) information in response packets returned from DHCP servers. If the information does not match the information it has for its own client (downstream) interface then the DHCP Relay Agent drops the packet. Note that [ip dhcp-relay agent-option](#) must be configured.

The DHCP Relay Agent Option 82 field is included in relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled ([ip dhcp-relay agent-option](#)), and
- DHCP Relay Agent is enabled on the device ([service dhcp-relay](#))

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay agent-option checking`  
`no ip dhcp-relay agent-option checking`

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Examples** To make the relay agent listening on eth0 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the relay agent from checking the DHCP Relay Agent Information Option (Option 82) field on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay agent-option checking
```

**Related commands** [ip dhcp-relay agent-option](#)  
[ip dhcp-relay agent-option remote-id](#)  
[ip dhcp-relay information policy](#)  
[service dhcp-relay](#)

# ip dhcp-relay agent-option remote-id

**Overview** Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field the DHCP Relay Agent inserts into clients' request packets. The Remote ID identifies the device that is inserting the DHCP Relay Agent Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the device's MAC address.

Use the **no** variant of this command to return the Remote ID for an interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay agent-option remote-id <remote-id>`  
`no ip dhcp-relay agent-option remote-id`

| Parameter                      | Description                                                                                                                                                      |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;remote-id&gt;</code> | An alphanumeric (ASCII) string, 1 to 63 characters in length. Additional characters allowed are hyphen (-), underscore (_) and hash (#). Spaces are not allowed. |

**Default** The Remote ID is set to the device's MAC address by default.

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled ([ip dhcp-relay agent-option](#)), and
- DHCP Relay Agent is enabled on the device ([service dhcp-relay](#))

**Examples** To set the Remote ID to myid for client DHCP packets received on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay agent-option remote-id
```

**Related commands** [ip dhcp-relay agent-option](#)  
[ip dhcp-relay agent-option checking](#)  
[show ip dhcp-relay](#)

# ip dhcp-relay information policy

**Overview** This command sets the policy for how the DHCP relay deals with packets arriving from the client that contain DHCP Relay Agent Option 82 information.

If the command **ip dhcp-relay agent-option** has not been configured, then this command has no effect at all - no alteration is made to Option 82 information in packets arriving from the client side.

However, if the command **ip dhcp-relay agent-option** has been configured, this command modifies how the DHCP relay service deals with cases where the packet arriving from the client side already contains DHCP Relay Agent Option 82 information.

This command sets the action that the DHCP relay should take when a received DHCP client request contains DHCP Relay Agent Option 82 information.

By default, the DHCP Relay Agent replaces any existing DHCP Relay Agent Option 82 field with its own DHCP Relay Agent field. This is equivalent to the functionality of the **replace** parameter.

The **no** variant of this command returns the policy to the default behavior - i.e. replacing the existing DHCP Relay Agent Option 82 field.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**NOTE:** The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands [ip dhcp-relay agent-option](#) and [ip dhcp-relay information policy](#) have been configured.

**Syntax** `ip dhcp-relay information policy {append|drop|keep|replace}`  
`no ip dhcp-relay information policy`

| Parameter | Description                                                                                                                                                    |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| append    | The DHCP Relay Agent appends the DHCP Relay Agent Option 82 field of the packet with its own DHCP Relay Agent Option 82 details.                               |
| drop      | The DHCP Relay Agent discards the packet.                                                                                                                      |
| keep      | The DHCP Relay Agent forwards the packet without altering the DHCP Relay Agent Option 82 field.                                                                |
| replace   | The DHCP Relay Agent replaces the existing DHCP Relay Agent details in the DHCP Relay Agent Option 82 field with its own details before forwarding the packet. |

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Examples** To make the DHCP Relay Agent listening on eth0 drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay information policy
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [service dhcp-server](#)

# ip dhcp-relay maxhops

**Overview** This command sets the hop count threshold for discarding BOOTP messages. When the hops field in a BOOTP message exceeds the threshold, the DHCP Relay Agent discards the BOOTP message. The hop count threshold is set to 10 hops by default.

Use the **no** variant of this command to reset the hop count to the default.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay maxhops <1-255>`  
`no ip dhcp-relay maxhops`

| Parameter | Description                  |
|-----------|------------------------------|
| <1-255>   | The maximum hop count value. |

**Default** The default hop count threshold is 10 hops.

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Example** To set the maximum number of hops to 5 for packets received on interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay maxhops 5
```

**Related commands** [service dhcp-relay](#)



# ip dhcp-relay max-message-length

**Overview** This command applies when the device is acting as a DHCP Relay Agent and DHCP Relay Agent Option 82 insertion is enabled. It sets the maximum DHCP message length (in bytes) for the DHCP packet with its DHCP Relay Agent Option 82 data inserted. From this value it calculates the maximum packet size that it will accept at its input. Packets that arrive greater than this value will be dropped.

The **no** variant of this command sets the maximum message length to its default of 1400 bytes.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay max-message-length <548-1472>`  
`no ip dhcp-relay max-message-length`

| Parameter  | Description                                                                                                 |
|------------|-------------------------------------------------------------------------------------------------------------|
| <548-1472> | The maximum DHCP message length (this is the message header plus the inserted DHCP option fields in bytes). |

**Default** The default is 1400 bytes.

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** When a DHCP Relay Agent (that has DHCP Relay Agent Option 82 insertion enabled) receives a request packet from a DHCP client, it will append the DHCP Relay Agent Option 82 component data, and forward the packet to the DHCP server. The DHCP client will sometimes issue packets containing pad option fields that can be overwritten with Option 82 data.

Where there are insufficient pad option fields to contain all the DHCP Relay Agent Option 82 data, the DHCP Relay Agent will increase the packet size to accommodate the DHCP Relay Agent Option 82 data. If the new (increased) packet size exceeds that defined by the **maximum-message-length** parameter, then the DHCP Relay Agent will drop the packet.

**NOTE:** Before setting this command, you must first run the [ip dhcp-relay agent-option](#) command. This will allow the DHCP Relay Agent Option 82 fields to be appended.

**Example** To set the maximum DHCP message length to 1200 bytes for packets arriving in interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay max-message-length 1200
```

To reset the maximum DHCP message length to the default of 1400 bytes for packets arriving in interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay max-message-length
```

**Related commands** [service dhcp-relay](#)

# ip dhcp-relay server-address

**Overview** This command adds a DHCP server for the DHCP Relay Agent to forward client DHCP packets to on a particular interface. You can add up to five DHCP servers on each device interface that the DHCP Relay Agent is listening on.

The **no** variant of this command deletes the specified DHCP server from the list of servers available to the DHCP relay agent.

The **no ip dhcp-relay** command removes all DHCP relay settings from the interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax**

```
ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}

no ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}

no ip dhcp-relay
```

| Parameter          | Description                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv4-address>     | Specify the IPv4 address of the DHCP server for the DHCP Relay Agent to forward client DHCP packets to, in dotted decimal notation. The IPv4 address uses the format A.B.C.D. |
| <ipv6-address>     | Specify the IPv6 address of the DHCPv6 server for the DHCPv6 Relay Agent to forward client DHCP packets to, in hexadecimal notation.                                          |
| <server-interface> | Specify the interface name of the DHCPv6 server. It is only required for a DHCPv6 server with an IPv6 address.                                                                |

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** For a DHCP server with an IPv6 address you must specify the interface for the DHCP server. See examples below for configuration differences between IPv4 and IPv6 DHCP relay servers.

See also the [service dhcp-relay](#) command to enable the DHCP Relay Agent on your device. The [ip dhcp-relay server-address](#) command defines a relay destination on an interface on the device, needed by the DHCP Relay Agent to relay DHCP client packets to a DHCP server.

**Examples: DHCP for IPv4** To enable the DHCP Relay Agent to relay DHCP packets on interface eth0 to the DHCP server with the IPv4 address 192.0.2.200, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay server-address 192.0.2.200
```

To remove the DHCP server with the IPv4 address 192.0.2.200 from the list of servers available to the DHCP Relay Agent on interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay server-address 192.0.2.200
```

**Examples: DHCPv6** To enable the DHCP Relay Agent on your device to relay DHCP packets on interface eth1.2 to the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface eth1.4, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface eth1.2
awplus(config-if)# ip dhcp-relay server-address
2001:0db8:010d::1 eth1.4
```

To remove the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface eth1.4 from the list of servers available to the DHCP Relay Agent on interface eth1.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
awplus(config-if)# no ip dhcp-relay server-address
2001:0db8:010d::1 eth1.4
```

**Example: disabling DHCP relay** To disable DHCP relay on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay
```

**Related commands** [service dhcp-relay](#)

# ip dhcp-relay short-lease

**Overview** Use this command to reduce the amount of time an IP address is assigned to a client device.

Long lease times can cause issues in dynamic networks where client devices frequently move between segments, such as VLANs. These device may retain an outdated IP address from its previous VLAN, disrupting communication.

This command is particularly useful in networks with a high turnover of devices or in environments where IP addresses are scarce.

Use the **no** variant of this command to remove the short lease time configuration.

**Syntax** `ip dhcp-relay short-lease <20-3600>`  
`no ip dhcp-relay short-lease`

| Parameter | Description                               |
|-----------|-------------------------------------------|
| <20-3600> | The lease time for DHCP relay in seconds. |

**Default** Not set

**Mode** Interface Configuration

**Example** To configure a DHCP Relay on interface vlan1 with a lease time of 200 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay short-lease 200
```

**Related commands** [show ip dhcp-relay](#)

**Command changes** Version 5.5.4-2.1: command added

# ip dhcp-relay use-client-side-address

**Overview** Use this command to configure DHCP-Relay to use the client-side interface (that is the interface receiving the DHCP client packets) IP address as the source address of the relayed DHCP packets.

Use the **no** variant of this command to disable the use of the client-side interface IP address as the source IP address for relayed DHCP packets.

**Syntax** `ip dhcp-relay use-client-side-address`  
`no ip dhcp-relay use-client-side-address`

| Parameter                            | Description                                                                                 |
|--------------------------------------|---------------------------------------------------------------------------------------------|
| <code>use-client-side-address</code> | Use the client side interface IP address as the source IP address for relayed DHCP packets. |

**Default** By default, the server-side interface IP address is used as the source IP address of DHCP relayed packets.

**Mode** Global Configuration

**Usage notes** In most cases, there are filters placed between the DHCP relay and DHCP server which only allow DHCP packets from the client subnet to the server and back. This command allows you to configure the DHCP relay so that the relay will use the IP address of the interface **receiving** clients' DHCP requests to be used as the source IP address of the relayed DHCP packets.

**Example** To configure the client-side IP address as the source IP address of DHCP relayed packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp-relay use-client-side-address
```

**Output** Figure 45-1: Example output from **show ip dhcp-relay**

The second line of the display output shows the status of the client-side address being enabled as the source IP address.

```
awplus#sh ip dhcp-relay

DHCP Relay Service is enabled
Use of client side address as source address is enabled
...
```

**Related commands** [ip dhcp-relay server-address](#)

**Command changes** Version 5.4.9-0.7: command added

# lease

**Overview** This command sets the expiration time for a leased address for the DHCP address pool you are configuring. The time set by the days, hours, minutes and seconds is cumulative. The minimum total lease time that can be configured is 20 seconds. The maximum total lease time that can be configured is 120 days.

Note that if you add a user-defined option 51 using the [option](#) command, then you will override any settings created with this command. Option 51 specifies a lease time of 1 day.

Use the **infinite** parameter to set the lease expiry time to infinite (leases never expire).

Use the **no** variant of this command to return the lease expiration time back to the default of one day.

**Syntax** `lease <days> <hours> <minutes> [<seconds>]`  
`lease infinite`  
`no lease`

| Parameter | Description                                                                                    |
|-----------|------------------------------------------------------------------------------------------------|
| <days>    | The number of days, from 0 to 120, that the lease expiry time is configured for.<br>Default: 1 |
| <hours>   | The number of hours, from 0 to 24, that the lease expiry time is configured for.<br>Default: 0 |
| <minutes> | The number of minutes, from 0 to 60, the lease expiry time is configured for.<br>Default: 0    |
| <seconds> | The number of seconds, from 0 to 60, the lease expiry time is configured for.                  |
| infinite  | The lease never expires.                                                                       |

**Default** The default lease time is 1 day.

**Mode** DHCP Configuration

**Examples** To set the lease expiration time for address pool P2 to 35 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# lease 0 0 35
```

To set the lease expiration time for the address pool `Nerv_Office` to 1 day, 5 hours, and 30 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# lease 1 5 30
```

To set the lease expiration time for the address pool `P3` to 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P3
awplus(dhcp-config)# lease 0 0 0 20
```

To set the lease expiration time for the pool to never expire, use the command:

```
awplus(dhcp-config)# lease infinite
```

To return the lease expiration time to the default of one day, use the command:

```
awplus(dhcp-config)# no lease
```

**Related  
commands**

[option](#)  
[service dhcp-server](#)  
[short-lease-threshold](#)



# network (DHCP)

**Overview** This command sets the network (subnet) that the DHCP address pool applies to. The **no** variant of this command removes the network (subnet) from the DHCP address pool.

**Syntax** `network`  
`{<ip-subnet-address/prefix-length>|<ip-subnet-address/mask>}`  
`no network`

| Parameter                                            | Description                                                                                                |
|------------------------------------------------------|------------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-subnet-address/prefix-length&gt;</code> | The IPv4 subnet address in dotted decimal notation followed by the prefix length in slash notation.        |
| <code>&lt;ip-subnet-address/mask&gt;</code>          | The IPv4 subnet address in dotted decimal notation followed by the subnet mask in dotted decimal notation. |

**Mode** DHCP Configuration

**Usage notes** This command will fail if it would make existing ranges invalid. For example, if they do not lie within the new network you are configuring.

The **no** variant of this command will fail if ranges still exist in the pool. You must remove all ranges in the pool before issuing a **no network** command to remove a network from the pool.

**Examples** To configure a network for the address pool P2, where the subnet is 192.0.2.5 and the mask is 255.255.255.0, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# network 192.0.2.5/24
```

or you can use dotted decimal notation instead of slash notation for the subnet-mask:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# network 192.0.2.5 255.255.255.0
```

**Related commands** [service dhcp-server](#)  
[subnet-mask](#)

## next-server

**Overview** This command sets the next server address for a DHCP server pool. It is the address of the next server that the client should use in its bootstrap process.

The **no** variant of this command removes the next server address from the DHCP address pool.

**Syntax** `next-server <ip-address>`  
`no next-server`

| Parameter                       | Description                                                |
|---------------------------------|------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code> | The server IP address, entered in dotted decimal notation. |

**Mode** DHCP Configuration

**Example** To set the next-server address for the address pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# next-server 192.0.2.2
```

# option

**Overview** This command adds a user-defined option to the DHCP address pool you are configuring. For the **hex**, **integer**, and **flag** option types, if the option already exists, the new option overwrites the existing option's value. Options with an **ip** type can hold a list of IP addresses or masks (i.e. entries that have the A.B.C.D address format), so if the option already exists in the pool, then the new IP address is added to the list of existing IP addresses.

Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

The **no** variant of this command removes the specified user-defined option from the DHCP pool, or all user-defined options from the DHCP pool.

**Syntax** `option [<1-254>|<option-name>] <option-value>`  
`no option [<1-254>|<option-value>]`

| Parameter      | Description                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-254>        | The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.                                                                 |
| <option-name>  | Option name associated with the option.                                                                                                                                                                |
| <option-value> | The option value. You must specify a value that is appropriate to the option type:                                                                                                                     |
|                | <b>hex</b> A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long. |
|                | <b>ip</b> An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually using the option command multiple times.   |
|                | <b>integer</b> A number from 0 to 4294967295.                                                                                                                                                          |
|                | <b>flag</b> A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag.                                                                                       |

**Mode** DHCP Configuration

**Examples** To add the ASCII-type option named `tftp-server-name` to the pool P2 and give the option the value `server1`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# option tftp-server-name server1
```

To add the hex-type option named `tcpip-node-type` to the pool P2 and give the option the value `08af`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# option tcpip-node-type 08af
```

To add multiple IP addresses for the ip-type option 175, use the command:

```
awplus(dhcp-config)# option 175 192.0.2.6
awplus(dhcp-config)# option 175 192.0.2.12
awplus(dhcp-config)# option 175 192.0.2.33
```

To add the option 179 to a pool, and give the option the value 123456, use the command:

```
awplus(dhcp-config)# option 179 123456
```

To add a user-defined flag option with the name `perform-router-discovery`, use the command:

```
awplus(dhcp-config)# option perform-router-discovery yes
```

To clear all user-defined options from a DHCP address pool, use the command:

```
awplus(dhcp-config)# no option
```

To clear a user-defined option, named `tftp-server-name`, use the command:

```
awplus(dhcp-config)# no option tftp-server-name
```

**Related  
commands**

[dns-server](#)

[ip dhcp option](#)

[lease](#)

[service dhcp-server](#)

[show ip dhcp pool](#)

# probe enable

**Overview** Use this command to enable lease probing for a DHCP pool. Probing is used by the DHCP server to check if an IP address it wants to lease to a client is already being used by another host.

The **no** variant of this command disables probing for a DHCP pool.

**Syntax** `probe enable`  
`no probe enable`

**Default** Probing is enabled by default.

**Mode** DHCP Pool Configuration

**Examples** To enable probing for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe enable
```

To disable probing for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe enable
```

**Related commands** [ip dhcp pool](#)  
[probe packets](#)  
[probe timeout](#)  
[probe type](#)  
[show ip dhcp pool](#)

# probe packets

**Overview** Use this command to specify the number of packets sent for each lease probe. Lease probing is configured on a per-DHCP pool basis. When set to 0 probing is effectively disabled.

The **no** variant of this command sets the number of probe packets sent to the default of 5.

**Syntax** `probe packets <0-10>`  
`no probe packets`

| Parameter | Description                       |
|-----------|-----------------------------------|
| <0-10>    | The number of probe packets sent. |

**Default** The default is 5.

**Mode** DHCP Pool Configuration

**Examples** To set the number of probe packets to 2 for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe packets 2
```

To set the number of probe packets to the default 5 for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe packets
```

**Related commands** [probe enable](#)  
[probe timeout](#)  
[probe type](#)  
[show ip dhcp pool](#)

# probe timeout

**Overview** Use this command to set the timeout value in milliseconds that the server waits for a response after each probe packet is sent. Lease probing is configured on a per-DHCP pool basis.

The **no** variant of this command sets the probe timeout value to the default setting, 200 milliseconds.

**Syntax** `probe timeout <50-5000>`  
`no probe timeout`

| Parameter                    | Description                       |
|------------------------------|-----------------------------------|
| <code>&lt;50-5000&gt;</code> | Timeout interval in milliseconds. |

**Default** The default timeout interval is 200 milliseconds.

**Mode** DHCP Pool Configuration

**Examples** To set the probe timeout value to 500 milliseconds for pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe timeout 500
```

To set the probe timeout value for pool P2 to the default, 200 milliseconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe timeout
```

**Related commands** [probe enable](#)  
[probe packets](#)  
[probe type](#)  
[show ip dhcp pool](#)

# probe type

**Overview** Use this command to set the probe type for a DHCP pool. The probe type specifies how the DHCP server checks whether an IP address is being used by other hosts, referred to as lease probing. If **arp** is specified, the server sends an ARP request to determine if an address is in use. If **ping** is specified, the server will send an ICMP Echo Request (ping).

The **no** variant of this command sets the probe type to the default setting, ping.

**Syntax** probe type {arp|ping}  
no probe type

| Parameter | Description       |
|-----------|-------------------|
| arp       | Probe using ARP.  |
| ping      | Probe using ping. |

**Default** The default probe type is ping.

**Mode** DHCP Pool Configuration

**Examples** To set the probe type to arp for the pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe type arp
```

To set the probe type for the pool P2 to the default, ping, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe type
```

**Related commands**

- [ip dhcp pool](#)
- [probe enable](#)
- [probe packets](#)
- [probe timeout](#)
- [show ip dhcp pool](#)



# range

**Overview** This command adds an address range to the DHCP address pool you are configuring. The DHCP server responds to client requests received from the pool's network. It assigns an IP addresses within the specified range. The IP address range must lie within the network. You can add multiple address ranges and individual IP addresses for a DHCP pool by using this command multiple times.

The **no** variant of this command removes an address range from the DHCP pool. Use the **no range all** command to remove all address ranges from the DHCP pool.

**Syntax** `range <ip-address> [<ip-address>]`  
`no range <ip-address> [<ip-address>]`  
`no range all`

| Parameter                       | Description                                                                                                                                                                                                                                |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code> | IPv4 address range for DHCP clients, in dotted decimal notation. The first IP address is the low end of the range, the second IP address is the high end. Specify only one IP address to add an individual IP address to the address pool. |

**Mode** DHCP Configuration

**Examples** To add an address range of 192.0.2.5 to 192.0.2.16 to the pool Nerv\_Office, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# range 192.0.2.5 192.0.2.16
```

To add the individual IP address 192.0.2.2 to a pool, use the command:

```
awplus(dhcp-config)# range 192.0.2.2
```

To remove all address ranges from a pool, use the command:

```
awplus(dhcp-config)# no range all
```

**Related commands** [ip dhcp pool](#)  
[service dhcp-server](#)  
[show ip dhcp pool](#)

# route

**Overview** This command allows the DHCP server to provide static routes to clients.

**Syntax** `route A.B.C.D/M A.B.C.D {both|opt249|rfc3442}`

| Parameter | Description                            |
|-----------|----------------------------------------|
| A.B.C.D/M | Subnet for the route                   |
| A.B.C.D   | Next hop for the route                 |
| both      | opt249 and rfc3442                     |
| opt249    | Classless static route option for DHCP |
| rfc3442   | Classless static route option for DHCP |

**Mode** DHCP Configuration

**Examples** To distribute static routes for route 0.0.0.0/0 whose next hop is 192.16.1.1 to clients using both opt249 and rfc3442, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool pubic
awplus(dhcp-config)# route 0.0.0.0/0 192.16.1.1 both
```

**Related commands** [ip dhcp pool](#)

# service dhcp-relay

**Overview** This command enables the DHCP Relay Agent on the device. However, on a given IP interface, no DHCP forwarding takes place until at least one DHCP server is specified to forward/relay all clients' DHCP packets to.

The **no** variant of this command disables the DHCP Relay Agent on the device for all interfaces.

**Syntax** `service dhcp-relay`  
`no service dhcp-relay`

**Mode** Global Configuration

**Usage notes** A maximum number of 400 DHCP Relay Agents (one per interface) can be configured on the device. Once this limit has been reached, any further attempts to configure DHCP Relay Agents will not be successful.

**Default** The DHCP-relay service is enabled by default.

**Examples** To enable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
```

To disable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# no service dhcp-relay
```

**Related commands** [ip dhcp-relay agent-option](#)  
[ip dhcp-relay agent-option checking](#)  
[ip dhcp-relay information policy](#)  
[ip dhcp-relay maxhops](#)  
[ip dhcp-relay server-address](#)

# service dhcp-server

**Overview** This command enables the DHCP server on your device. The server then listens for DHCP requests on all IP interfaces. It will not run if there are no IP interfaces configured.

The **no** variant of this command disables the DHCP server.

**Syntax** `service dhcp-server`  
`no service dhcp-server`

**Mode** Global Configuration

**Example** To enable the DHCP server, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-server
```

**Related commands** [ip dhcp pool](#)  
[show ip dhcp server summary](#)  
[subnet-mask](#)

# short-lease-threshold

**Overview** Use this command to configure a short lease threshold.

Use the **no** variant of this command to return the short lease threshold to the default of one minute.

**Syntax** `short-lease-threshold <hours> <minutes>`  
`no short-lease-threshold`

| Parameter                    | Description                          |
|------------------------------|--------------------------------------|
| <code>&lt;hours&gt;</code>   | The number of hours, from 0 to 24.   |
| <code>&lt;minutes&gt;</code> | The number of minutes, from 0 to 60. |

**Default** 1 minute.

**Mode** DHCP Configuration

**Usage notes** DHCP leases need to be backed up in NVS so that when the DHCP server reboots or goes through a power cycle it won't lose all the knowledge of these leases.

Some networks have a high number of mobile devices repeatedly requesting DHCP leases every few seconds before their existing lease expires. This can happen for example, when mobile devices move in and out of a Wi-Fi zone or when Wi-Fi signal strength changes. This means the same IP address can have multiple lease entries which can take up unnecessary backup file space.

The **short-lease-threshold** command allows you to configure the threshold for a short lease, from 1 minute to 24 hours. Any lease less than the threshold is deemed to be a short lease and will NOT be backed up to NVS.

This is useful if you have:

- limited backup file space, and
- you don't need to restore leases after a device reboot or power cycle

**Example** To set the short lease threshold for address pool P2 to 40 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# short-lease-threshold 0 40
```

To set the short lease threshold for address pool Nerv\_Office to 5 hours and 35 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# short-lease-threshold 5 35
```

To return the short lease threshold to the default of one minute, use the following commands:

```
awplus# configure terminal
awplus(config)# no short-lease-threshold
```

**Related  
commands**

[lease](#)

**Command  
changes**

Version 5.4.8-2.1: command added

# show counter dhcp-client

**Overview** This command shows counters for the DHCP client on your device.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show counter dhcp-client`

**Mode** User Exec and Privileged Exec

**Example** To display the message counters for the DHCP client on your device, use the command:

```
awplus# show counter dhcp-client
```

**Output** Figure 45-2: Example output from the **show counter dhcp-client** command

```
show counter dhcp-client

DHCPDISCOVER out 10
DHCPREQUEST out 34
DHCPDECLINE out 4
DHCPRELEASE out 0
DHCPPOFFER in 22
DHCPACK in 18
DHCPNAK in 0
```

**Table 1:** Parameters in the output of the **show counter dhcp-client** command

| Parameter        | Description                                                                  |
|------------------|------------------------------------------------------------------------------|
| DHCPDISCOVER out | The number of DHCP Discover messages sent by the client.                     |
| DHCPREQUEST out  | The number of DHCP Request messages sent by the client.                      |
| DHCPDECLINE out  | The number of DHCP Decline messages sent by the client.                      |
| DHCPRELEASE out  | The number of DHCP Release messages sent by the client.                      |
| DHCPPOFFER in    | The number of DHCP Offer messages received by the client.                    |
| DHCPACK in       | The number of DHCP Acknowledgement messages received by the client.          |
| DHCPNAK in       | The number of DHCP Negative Acknowledgement messages received by the client. |

**Related commands** [ip address dhcp](#)

# show counter dhcp-relay

**Overview** This command shows counters for the DHCP Relay Agent on your device.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show counter dhcp-relay`

**Mode** User Exec and Privileged Exec

**Examples** To display counters for the DHCP Relay Agent on your device, use the following command:

```
awplus# show counter dhcp-relay
```

**Output** Figure 45-3: Example output from the **show counter dhcp-relay** command

```
awplus#show counter dhcp-relay

DHCP relay counters
Requests In 4
Replies In 4
Relayed To Server 4
Relayed To Client 4
Out To Server Failed 0
Out To Client Failed 0
Invalid hlen 0
Bogus giaddr 0
Corrupt Agent Option 0
Missing Agent Option 0
Bad Circuit ID 0
Missing Circuit ID 0
Bad Remote ID 0
Missing Remote ID 0
Option Insert Failed 0
DHCPv6 Requests In 0
DHCPv6 Replies In 0
DHCPv6 Relayed to Server 0
DHCPv6 Relayed to Client 0
```

| Parameter         | Description                                                |
|-------------------|------------------------------------------------------------|
| Requests In       | The number of DHCP Request messages received from clients. |
| Replies In        | The number of DHCP Reply messages received from servers.   |
| Relayed To Server | The number of DHCP Request messages relayed to servers.    |
| Relayed To Client | The number of DHCP Reply messages relayed to clients.      |



| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Out To Server Failed | The number of failures when attempting to send request messages to servers. This is an internal debugging counter.                                                                                                                                                                                                                                                                                                                                                                 |
| Out To Client Failed | The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.                                                                                                                                                                                                                                                                                                                                                                   |
| Invalid hlen         | The number of incoming messages dropped due to an invalid hlen field.                                                                                                                                                                                                                                                                                                                                                                                                              |
| Bogus giaddr         | The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Corrupt Agent Option | The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command. |
| Missing Agent Option | The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command. |
| Bad Circuit ID       | The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.                               |
| Missing Circuit ID   | The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.                           |

| Parameter                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bad Remote ID            | The number of incoming DHCP Reply messages dropped due to a bad remote ID.<br>Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command                                                                                                                                                |
| Missing Remote ID        | The number of incoming DHCP Reply messages dropped due to a missing remote ID.<br>Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command                                                                                                                                            |
| Option Insert Failed     | The number of incoming DHCP Request messages dropped due to an error adding the DHCP Relay Agent information (option-82). This counter increments when: <ul style="list-style-type: none"> <li>the DHCP Relay Agent is set to drop packets with the DHCP Relay Agent Option 82 field already filled by another DHCP Relay Agent. This policy is set with the <code>ip dhcp-relay information policy</code> command.</li> <li>there is a packet error that stops the DHCP Relay Agent from being able to append the packet with its DHCP Relay Agent Information Option (Option 82) field.</li> </ul> |
| DHCPv6 Requests In       | The number of incoming DHCPv6 Request messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| DHCPv6 Replies In        | The number of incoming DHCPv6 Reply messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| DHCPv6 Relayed to Server | The number of DHCPv6 messages relayed to the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| DHCPv6 Relayed to Client | The number of DHCPv6 messages relayed to the client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

# show counter dhcp-server

**Overview** This command shows counters for the DHCP server on your device.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show counter dhcp-server`

**Mode** User Exec and Privileged Exec

**Example** To display counters for the DHCP server on your device, use the command:

```
awplus# show counter dhcp-server
```

**Output** Figure 45-4: Example output from the **show counter dhcp-server** command

|                      |       |    |
|----------------------|-------|----|
| DHCP server counters |       |    |
| DHCPDISCOVER in      | ..... | 20 |
| DHCPREQUEST in       | ..... | 12 |
| DHCPDECLINE in       | ..... | 1  |
| DHCPRELEASE in       | ..... | 0  |
| DHCPINFORM in        | ..... | 0  |
| DHCPOFFER out        | ..... | 8  |
| DHCPACK out          | ..... | 4  |
| DHCPNAK out          | ..... | 0  |
| BOOTREQUEST in       | ..... | 0  |
| BOOTREPLY out        | ..... | 0  |

**Table 2:** Parameters in the output of the **show counter dhcp-server** command

| Parameter       | Description                                                     |
|-----------------|-----------------------------------------------------------------|
| DHCPDISCOVER in | The number of Discover messages received by the DHCP server.    |
| DHCPREQUEST in  | The number of Request messages received by the DHCP server.     |
| DHCPDECLINE in  | The number of Decline messages received by the DHCP server.     |
| DHCPRELEASE in  | The number of Release messages received by the DHCP server.     |
| DHCPINFORM in   | The number of Inform messages received by the DHCP server.      |
| DHCPOFFER out   | The number of Offer messages sent by the DHCP server.           |
| DHCPACK out     | The number of Acknowledgement messages sent by the DHCP server. |

**Table 2:** Parameters in the output of the **show counter dhcp-server** command

| Parameter      | Description                                                                                                                                                                                                                                                                                                                     |
|----------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCPNAK out    | The number of Negative Acknowledgement messages sent by the DHCP server. The server sends these after receiving a request that it cannot fulfil because either there are no available IP addresses in the related address pool, or the request has come from a client that doesn't fit the network setting for an address pool. |
| BOOTREQUEST in | The number of bootp messages received by the DHCP server from bootp clients.                                                                                                                                                                                                                                                    |
| BOOTREPLY out  | The number of bootp messages sent by the DHCP server to bootp clients.                                                                                                                                                                                                                                                          |

**Related  
commands**

[service dhcp-server](#)  
[show ip dhcp binding](#)  
[show ip dhcp server statistics](#)  
[show ip dhcp pool](#)  
[show ip dhcp server statistics](#)

# show dhcp lease

**Overview** This command shows details about the leases that the DHCP client has acquired from a DHCP server for interfaces on the device.

For information on filtering and saving command output, see “Controlling “show” Command Output” in the [“Getting Started with AlliedWare\\_Plus” Feature Overview and Configuration Guide](#).

**Syntax** show dhcp lease [<interface>]

| Parameter   | Description                                       |
|-------------|---------------------------------------------------|
| <interface> | Interface name to display DHCP lease details for. |

**Mode** User Exec and Privileged Exec

**Example** To show the current lease expiry times for all interfaces, use the command:

```
awplus# show dhcp lease
```

To show the current lease for eth0, use the command:

```
awplus# show dhcp lease eth0
```

**Output** Figure 45-5: Example output from the **show dhcp lease eth0** command

|                        |                             |
|------------------------|-----------------------------|
| Interface eth0         |                             |
| -----                  |                             |
| IP Address:            | 192.168.22.4                |
| Expires:               | 13 Mar 2022 20:10:19        |
| Renew:                 | 13 Mar 2022 18:37:06        |
| Rebind:                | 13 Mar 2022 19:49:29        |
| Server:                |                             |
| Options:               |                             |
| subnet-mask            | 255.255.255.0               |
| routers                | 19.18.2.100,12.16.2.17      |
| dhcp-lease-time        | 3600                        |
| dhcp-message-type      | 5                           |
| domain-name-servers    | 192.168.100.50,19.88.200.33 |
| dhcp-server-identifier | 192.168.22.1                |
| domain-name            | alliedtelesis.com           |

**Related commands** [ip address dhcp](#)

# show ip dhcp binding

**Overview** This command shows the lease bindings that the DHCP server has allocated clients.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip dhcp binding [<ip-address>|<address-pool>]`

| Parameter                         | Description                                                                                                                        |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code>   | IPv4 address of a leased IP address, in dotted decimal notation. This displays the lease information for the specified IP address. |
| <code>&lt;address-pool&gt;</code> | Name of an address pool. This displays the lease information for all clients within the address pool.                              |

**Mode** User Exec and Privileged Exec

**Examples** To display all leases for every client in all address pools, use the command:

```
awplus# show ip dhcp binding
```

To display the details for the leased IP address 172.16.2.16, use the command:

```
awplus# show ip dhcp binding 172.16.2.16
```

To display the leases from the address pool MyPool, use the command:

```
awplus# show ip dhcp binding MyPool
```

**Output** Figure 45-6: Example output from the **show ip dhcp binding** command

| Pool 30_2_network Network 172.16.2.0/24 |                |         |                      |
|-----------------------------------------|----------------|---------|----------------------|
| DHCP Client Entries                     |                |         |                      |
| IP Address                              | ClientId       | Type    | Expiry               |
| 172.16.2.100                            | 0050.fc82.9ede | Dynamic | 21 Jun 2021 19:02:58 |
| 172.16.2.101                            | 000e.a6ae.7c14 | Static  | Infinite             |
| 172.16.2.102                            | 000e.a6ae.7c4c | Static  | Infinite             |
| 172.16.2.103                            | 000e.a69a.ac91 | Static  | Infinite             |
| 172.16.2.104                            | 00e0.189d.5e41 | Static  | Infinite             |
| 172.16.2.150                            | 00e0.2b04.5800 | Static  | Infinite             |
| 172.16.2.167                            | 4444.4400.35c3 | Dynamic | 21 Jun 2021 14:58:41 |

**Related commands**

- [clear ip dhcp binding](#)
- [ip dhcp pool](#)
- [lease](#)
- [range](#)

`service dhcp-server`  
`show ip dhcp pool`

# show ip dhcp pool

**Overview** This command displays the configuration details and system usage of the DHCP address pools configured on the device.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip dhcp pool [<address-pool>]`

| Parameter      | Description                                                                                          |
|----------------|------------------------------------------------------------------------------------------------------|
| <address-pool> | Name of a specific address pool. This displays the configuration of the specified address pool only. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ip dhcp pool`

**Output** Figure 45-7: Example output from the **show ip dhcp pool** command

```
Pool p1 :
 network: 192.168.1.0/24
 address ranges:
 addr: 192.168.1.10 to 192.168.1.18
 static host addresses:
 addr: 192.168.1.12 MAC addr: 1111.2222.3333
 lease <days:hours:minutes:seconds> <1:0:0:0>
 subnet mask: 255.255.255.0 (pool's network mask)
 Probe: Default Values
 Status: Enabled [Enabled]
 Type: ARP [Ping]
 Packets: 2 [5]
 Timeout: 200 msec [200]
 Dynamic addresses:
 Total: 8
 Leased: 2
 Utilization: 25.0 %
 Static host addresses:
 Total: 1
 Leased: 1
```



**Output** Figure 45-8: Example output from the **show ip dhcp pool** command with IP address 192.168.1.12 assigned to a VLAN interface on the device:

```
Pool p1 :
network: 192.168.1.0/24
address ranges:
 addr: 192.168.1.10 to 192.168.1.18
 (interface addr 192.168.1.12 excluded)
 (static host addr 192.168.1.12 excluded)
static host addresses:
 addr: 192.168.1.12 MAC addr: 1111.2222.3333
 (= interface addr, so excluded)
lease <days:hours:minutes:seconds> <1:0:0:0>
subnet mask: 255.255.255.0 (pool's network mask)
Probe: Default Values
 Status: Enabled [Enabled]
 Type: ARP [Ping]
 Packets: 2 [5]
 Timeout: 200 msec [200]
Dynamic addresses:
 Total: 8
 Leased: 2
 Utilization: 25.0 %
Static host addresses:
 Total: 1
 Leased: 1
```

**Output** Figure 45-9: Example output from the **show ip dhcp pool** command when a host with MAC 0000.cd38.05f9 is registered as a static host by DHCP Framed IP Lease feature from AUTHD:

```
Pool p1 :
 network: 10.1.1.0/24
 address ranges:
 addr: 10.1.1.101 to 10.1.1.199
 (static host addr 10.1.1.122 excluded)
 (static host addr 10.1.1.111 excluded)
 static host addresses:
 addr: 10.1.1.122 MAC addr: 0000.1111.2222
 addr: 10.1.1.111 MAC addr: 0000.cd38.05f9
 Netmask : 255.255.255.0
 Gateway : 10.1.1.1
 Lease : 60 seconds
 Added by AUTHD

 lease <1:0:0:0>
 subnet mask: 255.255.255.0 (pool's network mask)
 Probe: Default Values
 Status: Enabled [Enabled]
 Type: Ping [Ping]
 Packets: 5 [5]
 Timeout: 200 msec [200]
 Dynamic addresses:
 Total: 97
 Leased: 1
 Utilization: 1.0 %
 Static host addresses:
 Total: 2
 Leased: 2
```

Table 45-1: Parameters in the output of **show ip dhcp pool**

| Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pool           | Name of the pool.                                                                                                                                                                                                                                                                                                                                                                                     |
| network        | Subnet and mask length of the pool.                                                                                                                                                                                                                                                                                                                                                                   |
| address ranges | Individual IP addresses and address ranges configured for the pool. The DHCP server can offer clients an IP address from within the specified ranges only.<br>Any of these addresses that match an interface address on the device, or a static host address configured in the pool, will be automatically excluded from the range, and a message to this effect will appear beneath the range entry. |

Table 45-1: Parameters in the output of **show ip dhcp pool** (cont.)

| Parameter                          | Description                                                                                                                                                                                                                                                                                                         |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| static host addresses              | The static host addresses configured on the pool. Each IP address is permanently assigned to the client with the matching MAC address. Any of these addresses that match an interface address on the device will be automatically excluded, and a message to this effect will appear beneath the static host entry. |
| lease<br><days:hours:minutes>      | The lease duration for address allocated by this pool.                                                                                                                                                                                                                                                              |
| domain                             | The domain name sent by the pool to clients. This is the domain name that the client should use when resolving host names using DNS.                                                                                                                                                                                |
| subnet mask                        | The subnet mask sent by the pool to clients.                                                                                                                                                                                                                                                                        |
| Probe - Status                     | Whether lease probing is enabled or disabled.                                                                                                                                                                                                                                                                       |
| Probe - Type                       | The lease probe type configured. Either ping or ARP.                                                                                                                                                                                                                                                                |
| Probe - Packets                    | The number of packets sent for each lease probe in the range 0 to 10.                                                                                                                                                                                                                                               |
| Probe - Timeout                    | The timeout value in milliseconds to wait for a response after each probe packet is sent. In the range 50 to 5000.                                                                                                                                                                                                  |
| dns servers                        | The DNS server addresses sent to by the pool to clients.                                                                                                                                                                                                                                                            |
| default-router(s)                  | The default router addresses sent by the pool to clients.                                                                                                                                                                                                                                                           |
| user-defined options               | The list of user-defined options sent by the pool to clients.                                                                                                                                                                                                                                                       |
| Dynamic addresses-<br>Total        | The total number of IP addresses that have been configured in the pool for dynamic allocation to DHCP clients.                                                                                                                                                                                                      |
| Dynamic addresses-<br>Leased       | The number of IP addresses in the pool that have been dynamically allocated (leased) to DHCP clients.                                                                                                                                                                                                               |
| Dynamic addresses -<br>Utilization | The percentage of IP addresses in the pool that are currently dynamically allocated to clients.                                                                                                                                                                                                                     |
| Static host addresses-<br>Total    | The number of static IP addresses configured in the pool for specific DHCP client hosts.                                                                                                                                                                                                                            |
| Static host addresses<br>- Leased  | The number of static IP addresses assigned to specific DHCP client hosts.                                                                                                                                                                                                                                           |

**Related commands**

- [ip dhcp pool](#)
- [probe enable](#)
- [probe packets](#)
- [probe timeout](#)
- [probe type](#)
- [range](#)
- [service dhcp-server](#)
- [subnet-mask](#)

# show ip dhcp-relay

**Overview** This command shows the configuration of the DHCP Relay Agent on each interface.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip dhcp-relay [interface <interface-name>]`

| Parameter        | Description                                                                                          |
|------------------|------------------------------------------------------------------------------------------------------|
| <interface-name> | Name of a specific interface. This displays the DHCP configuration for the specified interface only. |

**Mode** User Exec and Privileged Exec

**Example** To display the DHCP Relay Agent’s configuration on the interface eth0, use the command:

```
awplus# show ip dhcp-relay interface eth0
```

**Output** Figure 45-10: Example output from the **show ip dhcp-relay** command

```
DHCP Relay Service is enabled

eth0 is up, line protocol is up
Maximum hop count is 10
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
The Remote Id string for Relay Agent Option is 0000.cd28.074c
Relay information policy is to append new relay agent
information
List of servers : 192.168.1.200
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [ip dhcp-relay information policy](#)
- [ip dhcp-relay maxhops](#)
- [ip dhcp-relay server-address](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# show ip dhcp server statistics

**Overview** This command shows statistics related to the DHCP server.

You can display the server counters using the [show counter dhcp-server](#) command as well as with this command.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show ip dhcp server statistics

**Mode** User Exec and Privileged Exec

**Example** To display the server statistics, use the command:

```
awplus# show ip dhcp server statistics
```

**Output** Figure 45-11: Example output from the **show ip dhcp server statistics** command

|                         |       |    |
|-------------------------|-------|----|
| DHCP server counters    |       |    |
| DHCPDISCOVER in         | ..... | 20 |
| DHCPREQUEST in          | ..... | 12 |
| DHCPDECLINE in          | ..... | 1  |
| DHCPRELEASE in          | ..... | 0  |
| DHCPINFORM in           | ..... | 0  |
| DHCPOFFER out           | ..... | 8  |
| DHCPACK out             | ..... | 4  |
| DHCPNAK out             | ..... | 0  |
| BOOTREQUEST in          | ..... | 0  |
| BOOTREPLY out           | ..... | 0  |
| DHCPLEASEQUERY in       | ..... | 0  |
| DHCPLEASEUNKNOWN out    | ..... | 0  |
| DHCPLEASEACTIVE out     | ..... | 0  |
| DHCPLEASEUNASSIGNED out | ..... | 0  |

| Parameter       | Description                                                  |
|-----------------|--------------------------------------------------------------|
| DHCPDISCOVER in | The number of Discover messages received by the DHCP server. |
| DHCPREQUEST in  | The number of Request messages received by the DHCP server.  |
| DHCPDECLINE in  | The number of Decline messages received by the DHCP server.  |
| DHCPRELEASE in  | The number of Release messages received by the DHCP server.  |

| Parameter               | Description                                                                                                                                                                                                                                                                                                                     |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| DHCPINFORM in           | The number of Inform messages received by the DHCP server.                                                                                                                                                                                                                                                                      |
| DHCPOFFER out           | The number of Offer messages sent by the DHCP server.                                                                                                                                                                                                                                                                           |
| DHCPACK out             | The number of Acknowledgement messages sent by the DHCP server.                                                                                                                                                                                                                                                                 |
| DHCPNAK out             | The number of Negative Acknowledgement messages sent by the DHCP server. The server sends these after receiving a request that it cannot fulfil because either there are no available IP addresses in the related address pool, or the request has come from a client that doesn't fit the network setting for an address pool. |
| BOOTREQUEST in          | The number of bootp messages received by the DHCP server from bootp clients.                                                                                                                                                                                                                                                    |
| BOOTREPLY out           | The number of bootp messages sent by the DHCP server to bootp clients.                                                                                                                                                                                                                                                          |
| DHCPLEASEQUERY in       | The number of Lease Query messages received by the DHCP server from DHCP Relay Agents.                                                                                                                                                                                                                                          |
| DHCPLEASEUNKNOWN out    | The number of Lease Unknown messages sent by the DHCP server to DHCP Relay Agents.                                                                                                                                                                                                                                              |
| DHCPLEASEACTIVE out     | The number of Lease Active messages sent by the DHCP server to DHCP Relay Agents.                                                                                                                                                                                                                                               |
| DHCPLEASEUNASSIGNED out | The number of Lease Unassigned messages sent by the DHCP server to DHCP Relay Agents.                                                                                                                                                                                                                                           |

**Related commands**

- [show counter dhcp-server](#)
- [service dhcp-server](#)
- [show ip dhcp binding](#)
- [show ip dhcp pool](#)

# show ip dhcp server summary

**Overview** This command shows the current configuration of the DHCP server. This includes:

- whether the DHCP server is enabled
- whether the DHCP server is configured to ignore BOOTP requests
- whether the DHCP server is configured to support DHCP lease queries
- the details of any user-defined options
- a list of the names of all DHCP address pools currently configured

This show command does not include any configuration details of the address pools. You can display these using the [show ip dhcp pool](#) command.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip dhcp server summary`

**Mode** User Exec and Privileged Exec

**Example** To display the current configuration of the DHCP server, use the command:

```
awplus# show ip dhcp server summary
```

**Output** Figure 45-12: Example output from the **show ip dhcp server summary** command

```
DHCP Server service is disabled
BOOTP ignore is disabled
DHCP leasequery support is disabled
Pool list: p2
```

**Related commands**

- [ip dhcp leasequery enable](#)
- [ip dhcp pool](#)
- [service dhcp-server](#)



# subnet-mask

**Overview** This command sets the subnet mask option for a DHCP address pool you are configuring. Use this command to specify the client's subnet mask as defined in RFC 950. This sets the subnet details using the pre-defined option 1. Note that if you create a user-defined option 1 using the [option](#) command, then you will override any settings created with this command. If you do not specify a subnet mask using this command, then the pool's network mask (specified using the [next-server](#) command) is applied.

The **no** variant of this command removes a subnet mask option from a DHCP pool. The pool reverts to using the pool's network mask.

**Syntax** `subnet-mask <mask>`  
`no subnet-mask`

| Parameter                 | Description                                         |
|---------------------------|-----------------------------------------------------|
| <code>&lt;mask&gt;</code> | Valid IPv4 subnet mask, in dotted decimal notation. |

**Mode** DHCP Configuration

**Examples** To set the subnet mask option to 255.255.255.0 for DHCP pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# subnet-mask 255.255.255.0
```

To remove the subnet mask option from DHCP pool P2, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no subnet-mask
```

**Related commands**

- [default-router](#)
- [dns-server](#)
- [domain-name](#)
- [next-server](#)
- [option](#)
- [service dhcp-server](#)
- [show ip dhcp pool](#)

# 46

# DHCP for IPv6 (DHCPv6) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure DHCPv6. For more information, see the [DHCPv6 Feature Overview and Configuration Guide](#).

DHCPv6 is a network protocol used to configure IPv6 hosts with IPv6 addresses and IPv6 prefixes for an IPv6 network. DHCPv6 is used instead of SLAAC (Stateless Address Autoconfiguration) at sites where centralized management of IPv6 hosts is needed. IPv6 routers require automatic configuration of IPv6 addresses and IPv6 prefixes.

DHCPv6 Prefix Delegation provides automatic configuration of IPv6 addresses and IPv6 prefixes.

Note that DHCPv6 client does not support tunnel interface.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**NOTE:** The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.

- Command List**
- [“address prefix”](#) on page 2232
  - [“address range”](#) on page 2234
  - [“clear counter ipv6 dhcp-client”](#) on page 2236
  - [“clear counter ipv6 dhcp-server”](#) on page 2237
  - [“clear ipv6 dhcp binding”](#) on page 2238
  - [“clear ipv6 dhcp client”](#) on page 2240
  - [“dns-server \(DHCPv6\)”](#) on page 2241
  - [“domain-name \(DHCPv6\)”](#) on page 2243

- ["ip dhcp-relay agent-option"](#) on page 2244
- ["ip dhcp-relay agent-option checking"](#) on page 2246
- ["ip dhcp-relay agent-option remote-id"](#) on page 2247
- ["ip dhcp-relay information policy"](#) on page 2248
- ["ip dhcp-relay maxhops"](#) on page 2250
- ["ip dhcp-relay max-message-length"](#) on page 2251
- ["ip dhcp-relay server-address"](#) on page 2253
- ["ip dhcp-relay short-lease-ipv6"](#) on page 2255
- ["ipv6 address \(DHCPv6 PD\)"](#) on page 2256
- ["ipv6 address dhcp"](#) on page 2258
- ["ipv6 dhcp client pd"](#) on page 2260
- ["ipv6 dhcp option"](#) on page 2262
- ["ipv6 dhcp pool"](#) on page 2264
- ["ipv6 dhcp server"](#) on page 2266
- ["ipv6 local pool"](#) on page 2267
- ["ipv6 nd prefix \(DHCPv6\)"](#) on page 2269
- ["link-address"](#) on page 2271
- ["option \(DHCPv6\)"](#) on page 2273
- ["prefix-delegation pool"](#) on page 2275
- ["service dhcp-relay"](#) on page 2277
- ["show counter dhcp-relay"](#) on page 2278
- ["show counter ipv6 dhcp-client"](#) on page 2281
- ["show counter ipv6 dhcp-server"](#) on page 2283
- ["show ip dhcp-relay"](#) on page 2285
- ["show ipv6 dhcp"](#) on page 2286
- ["show ipv6 dhcp binding"](#) on page 2287
- ["show ipv6 dhcp interface"](#) on page 2290
- ["show ipv6 dhcp pool"](#) on page 2292
- ["sntp-address"](#) on page 2294

# address prefix

**Overview** Use this command in DHCPv6 Configuration mode to specify an address prefix for address assignment with DHCPv6 server pool configuration.

Use the **no** variant of this command to remove the address prefix from the DHCPv6 server pool.

**Syntax** address prefix <ipv6-prefix/prefix-length> [lifetime {<valid-time>|infinite} {<preferred-time>|infinite}]  
no address prefix <ipv6-prefix/prefix-length>

| Parameter                   | Description                                                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv6-prefix/prefix-length> | Specify an IPv6 prefix and prefix length. The prefix length indicates the length of the IPv6 prefix assigned to the pool. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.                                                                                                                                                                             |
| lifetime                    | Specify a time period for the hosts to remember router advertisements (RAs).<br>If you specify the optional lifetime parameter with this command then you must also specify a <i>valid-time</i> and a <i>preferred-time</i> value.<br>See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry. |
| <valid-time>                | Specify a valid lifetime in seconds in the range <5-315360000>.<br>The default valid lifetime is 2592000 seconds.                                                                                                                                                                                                                                                                                                 |
| infinite                    | Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.                                                                                                                                                                                                                                                                                                           |
| <preferred-time>            | Specify a preferred lifetime in seconds in the range <5-315360000>.<br>The default preferred lifetime is 604800 seconds.                                                                                                                                                                                                                                                                                          |

**Mode** DHCPv6 Configuration

**Default** The default valid lifetime is 2592000 seconds and the default preferred lifetime is 604800 seconds.

**Usage notes** This command creates a pool of prefixes from which addresses are assigned to clients on request, and allocates a network prefix from which the DHCPv6 Server leases addresses. This command is an alternative to using a range set using the [address range](#) command.

The DHCPv6 Server selects an IPv6 address from the range available allocated by the IPv6 prefix, randomly generating the suffix of the IPv6 address, with the specified preferred and valid lifetime leases. Leased IPv6 address are found in the

DHCPv6 Server REPLY packet, which is located within the IANA (Identity Association for Non-temporary Addresses) IA address field in the **REPLY** message.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Examples** To add IPv6 address prefix 2001:0db8:1::/48 for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# address prefix 2001:0db8:1::/48
```

To remove a configured IPv6 address prefix for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# no address prefix 2001:0db8:1::/48
```

**Related commands** [address range](#)  
[ipv6 dhcp pool](#)

**Validation Commands** [show ipv6 dhcp binding](#)  
[show ipv6 dhcp pool](#)

# address range

**Overview** Use this command in DHCPv6 Configuration mode to specify an address range for address assignment with DHCPv6 server pool configuration.

Use the **no** variant of this command to remove an address range from the DHCPv6 server pool.

**Syntax** `address range <first-ipv6-address>  
<last-ipv6-address>[lifetime {<valid-time>|infinite}  
{<preferred-time>|infinite}]`  
`no address range <first-ipv6-address> <last-ipv6-address>`

| Parameter                               | Description                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;first-ipv6-address&gt;</code> | Specify the first IPv6 address of the IPv6 address range, in hexadecimal notation in the format <code>X:X::X:X</code> .                                                                                                                                                                                                                                                                  |
| <code>&lt;last-ipv6-address&gt;</code>  | Specify the last IPv6 address of the IPv6 address range, in hexadecimal notation in the format <code>X:X::X:X</code> .                                                                                                                                                                                                                                                                   |
| <code>lifetime</code>                   | Optional. Specify a time period for the hosts to remember router advertisements (RAs).<br>If you specify this parameter then you must also specify a <i>valid-time</i> and a <i>preferred-time</i> value.<br>See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry. |
| <code>&lt;valid-time&gt;</code>         | Specify a valid lifetime in seconds in the range <code>&lt;5-31536000&gt;</code> .<br>The default valid lifetime is 2592000 seconds.                                                                                                                                                                                                                                                     |
| <code>infinite</code>                   | Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.                                                                                                                                                                                                                                                                                  |
| <code>&lt;preferred-time&gt;</code>     | Specify a preferred lifetime in seconds in the range <code>&lt;5-31536000&gt;</code> .<br>The default preferred lifetime is 604800 seconds.                                                                                                                                                                                                                                              |

**Default** The default valid lifetime is 2592000 seconds and the default preferred lifetime is 604800 seconds.

**Mode** DHCPv6 Configuration

**Usage** Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Examples** To add the IPv6 address range 2001:0db8:1::1 to 2001:0db8:1fff::1 for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# address range 2001:0db8:1::1
2001:0db8:1fff::1
```

To remove a configured IPv6 address range for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# no address range
```

**Related commands** [address prefix](#)  
[ipv6 dhcp pool](#)

**Validation Commands** [show ipv6 dhcp binding](#)  
[show ipv6 dhcp pool](#)

# clear counter ipv6 dhcp-client

**Overview** Use this command in Privileged Exec mode to clear DHCPv6 client counters.

**Syntax** `clear counter ipv6 dhcp-client`

**Mode** Privileged Exec

**Example** To clear DHCPv6 client counters, use the following command:

```
awplus# clear counter ipv6 dhcp-client
```

**Related commands** [show counter ipv6 dhcp-client](#)



# clear counter ipv6 dhcp-server

**Overview** Use this command in Privileged Exec mode to clear DHCPv6 server counters.

**Syntax** `clear counter ipv6 dhcp-server`

**Mode** Privileged Exec

**Example** To clear DHCPv6 server counters, use the following command:

```
awplus# clear counter ipv6 dhcp-server
```

**Related commands** [show counter ipv6 dhcp-server](#)

# clear ipv6 dhcp binding

**Overview** Use this command in Privileged Exec mode to clear either a specific lease binding or the lease bindings as specified by the command parameters. The command will only take effect on dynamically allocated bindings, not statically configured bindings. This command clears binding entries on the DHCPv6 server binding table.

**Syntax** `clear ipv6 dhcp binding {ipv6 <prefix>|duid <DUID>|all|pool <name>}`

| Parameter     | Description                                                                                                                                                                          |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ipv6 <prefix> | Optional. Specify the IPv6 prefix of the DHCPv6 client, in hexadecimal notation in the format X:X:X:X.                                                                               |
| duid <DUID>   | Specify the DUID (DHCPv6 unique ID) of the DHCPv6 client.                                                                                                                            |
| all           | All DHCPv6 bindings.                                                                                                                                                                 |
| pool <name>   | Description used to identify DHCPv6 server address pool. Valid characters are any printable character. If the name contains spaces then you must enclose these in "quotation marks". |

**Mode** Privileged Exec

**Usage notes** A specific binding may be deleted by **ipv6** address or **duid** address, or several bindings may be deleted at once using **all** or **pool**.

Note that if you specify to clear the **ipv6** or **duid** address of what is actually a static DHCPv6 binding, an error message is displayed. If **all** or **pool** are specified and one or more static DHCPv6 bindings exist within those addresses, any dynamic entries within those addresses are cleared but any static entries are not cleared.

The clear ipv6 dhcp binding command is used as a server function. A binding table entry on the DHCPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding, all prefix lifetimes have expired, or when a user runs the clear ipv6 dhcp binding command.

If the **clear ipv6 dhcp binding** command is used with the optional IPv6 address parameter, only the binding for the specified client is deleted. If the **clear ipv6 dhcp binding** command is used without the optional IPv6 address parameter, then all automatic client bindings are deleted from the DHCPv6 bindings table.

**Example** To clear all dynamic DHCPv6 server binding entries, use the command:

```
awplus# clear ipv6 dhcp binding all
```

**Output** Figure 46-1: Example output from the **clear ipv6 dhcp binding all** command

```
awplus#clear ipv6 dhcp binding all
% Deleted 1 entries
```

**Related commands** [show ipv6 dhcp binding](#)

# clear ipv6 dhcp client

**Overview** Use this command in Privileged Exec mode to restart a DHCPv6 client on an interface.

**Syntax** `clear ipv6 dhcp client <interface>`

| Parameter                      | Description                                               |
|--------------------------------|-----------------------------------------------------------|
| <code>&lt;interface&gt;</code> | Specify the interface name to restart a DHCPv6 client on. |

**Mode** Privileged Exec

**Example** To restart a DHCPv6 client on interface eth0, use the following command:

```
awplus# clear ipv6 dhcp client eth0
```

**Related commands** [show ipv6 dhcp binding](#)

# dns-server (DHCPv6)

**Overview** Use this command to add a Domain Name System (DNS) server to the DHCPv6 address pool you are configuring. You can use this command multiple times to create a list of DNS name servers available to the client. This sets the DNS server details using the pre-defined option 6. Note that if you add a user-defined option 6 using the [option \(DHCPv6\)](#) command, then you will override any settings created with this command.

Use the **no** variant of this command to remove either the specified DNS server or all DNS servers from the DHCPv6 pool.

**Syntax** `dns-server <ipv6-address>`  
`no dns-server [<ipv6-address>]`

| Parameter                         | Description                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-address&gt;</code> | Specify an IPv6 address of the DNS server, in hexadecimal notation in the format <code>X:X::X:X</code> . This parameter is required when adding a DNS server to the DHCPv6 address pool. All DNS servers are removed from the DHCPv6 pool if you enter the <code>no dns-server</code> command without this parameter. |

**Mode** DHCPv6 Configuration

**Examples** To add the DNS server with the assigned IPv6 address `2001:0db8:3000:3000::32` to the DHCPv6 server pool named `P2`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# dns-server 2001:0db8:3000:3000::32
```

To remove the DNS server with the assigned IPv6 address `2001:0db8:3000:3000::32` from the DHCPv6 server pool named `P2`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no dns-server 2001:0db8:3000:3000::32
```

To remove all DNS servers from the DHCPv6 server pool named `P2`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no dns-server
```

**Related  
commands**    `ipv6 dhcp pool`  
                  `option (DHCPv6)`  
                  `show ipv6 dhcp pool`

# domain-name (DHCPv6)

**Overview** Use this command in DHCPv6 Configuration mode to add a domain name to the DHCPv6 server address pool you are configuring.

Use the **no** variant of this command to remove a domain name from the address pool.

**Syntax** `domain-name <domain-name>`  
`no domain-name`

| Parameter                        | Description                                                                                                                                                                                      |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;domain-name&gt;</code> | Specify the domain name you wish to assign the DHCPv6 server address pool. Valid characters are printable characters. If the name contains spaces then you must enclose it in "quotation marks". |

**Mode** DHCPv6 Configuration

**Usage** This command specifies the domain name that a client should use when resolving host names using the Domain Name System, and sets the domain name details using the pre-defined option 15. Note that if you add a user-defined option 15 using the [option \(DHCPv6\)](#) command, then you will override any settings created with this command.

**Examples** To add the domain name `Engineering` to DHCPv6 server pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# domain-name Engineering
```

To remove the domain name `Engineering` from DHCPv6 server pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no domain-name Engineering
```

**Related commands** [dns-server \(DHCPv6\)](#)  
[option \(DHCPv6\)](#)  
[show ipv6 dhcp pool](#)

# ip dhcp-relay agent-option

**Overview** This command enables the DHCP Relay Agent to insert the DHCP Relay Agent Information Option (Option 82) into the client-request packets that it relays to its DHCP server. This allows the DHCP Relay Agent to pass on information to the server about the network location of the client device. The DHCP Relay Agent strips the DHCP Relay Agent Option 82 field out of the DHCP server's response, so that the DHCP client never sees this field.

When the DHCP Relay Agent appends its DHCP Relay Agent Option 82 data into the packet, it first overwrites any pad options present; then if necessary, it increases the packet length to accommodate the DHCP Relay Agent Option 82 data.

The **no** variant of this command stops the DHCP Relay Agent from appending the Option 82 field onto DHCP requests before forwarding it to the server.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**NOTE:** The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands [ip dhcp-relay agent-option](#) and [ip dhcp-relay information policy](#) have been configured.

**Syntax** `ip dhcp-relay agent-option`  
`no ip dhcp-relay agent-option`

**Default** DHCP Relay Agent Information Option (Option 82) insertion is disabled by default.

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** Use this command to alter the DHCP Relay Agent Option 82 setting when your device is the first hop for the DHCP client. To limit the maximum length of the packet, use the [ip dhcp-relay max-message-length](#) command.

**Examples** To make the relay agent listening on eth0 append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the relay agent from appending the DHCP Relay Agent Option 82 field on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay agent-option
```



**Related commands**

- [ip dhcp-relay agent-option remote-id](#)
- [ip dhcp-relay information policy](#)
- [ip dhcp-relay max-message-length](#)
- [service dhcp-relay](#)

# ip dhcp-relay agent-option checking

**Overview** This command enables the DHCP Relay Agent to check DHCP Relay Agent Information Option (Option 82) information in response packets returned from DHCP servers. If the information does not match the information it has for its own client (downstream) interface then the DHCP Relay Agent drops the packet. Note that [ip dhcp-relay agent-option](#) must be configured.

The DHCP Relay Agent Option 82 field is included in relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled ([ip dhcp-relay agent-option](#)), and
- DHCP Relay Agent is enabled on the device ([service dhcp-relay](#))

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay agent-option checking`  
`no ip dhcp-relay agent-option checking`

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Examples** To make the relay agent listening on eth0 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the relay agent from checking the DHCP Relay Agent Information Option (Option 82) field on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay agent-option checking
```

**Related commands** [ip dhcp-relay agent-option](#)  
[ip dhcp-relay agent-option remote-id](#)  
[ip dhcp-relay information policy](#)  
[service dhcp-relay](#)

# ip dhcp-relay agent-option remote-id

**Overview** Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field the DHCP Relay Agent inserts into clients' request packets. The Remote ID identifies the device that is inserting the DHCP Relay Agent Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the device's MAC address.

Use the **no** variant of this command to return the Remote ID for an interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay agent-option remote-id <remote-id>`  
`no ip dhcp-relay agent-option remote-id`

| Parameter                      | Description                                                                                                                                                      |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;remote-id&gt;</code> | An alphanumeric (ASCII) string, 1 to 63 characters in length. Additional characters allowed are hyphen (-), underscore (_) and hash (#). Spaces are not allowed. |

**Default** The Remote ID is set to the device's MAC address by default.

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled ([ip dhcp-relay agent-option](#)), and
- DHCP Relay Agent is enabled on the device ([service dhcp-relay](#))

**Examples** To set the Remote ID to myid for client DHCP packets received on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay agent-option remote-id
```

**Related commands** [ip dhcp-relay agent-option](#)  
[ip dhcp-relay agent-option checking](#)  
[show ip dhcp-relay](#)

# ip dhcp-relay information policy

**Overview** This command sets the policy for how the DHCP relay deals with packets arriving from the client that contain DHCP Relay Agent Option 82 information.

If the command **ip dhcp-relay agent-option** has not been configured, then this command has no effect at all - no alteration is made to Option 82 information in packets arriving from the client side.

However, if the command **ip dhcp-relay agent-option** has been configured, this command modifies how the DHCP relay service deals with cases where the packet arriving from the client side already contains DHCP Relay Agent Option 82 information.

This command sets the action that the DHCP relay should take when a received DHCP client request contains DHCP Relay Agent Option 82 information.

By default, the DHCP Relay Agent replaces any existing DHCP Relay Agent Option 82 field with its own DHCP Relay Agent field. This is equivalent to the functionality of the **replace** parameter.

The **no** variant of this command returns the policy to the default behavior - i.e. replacing the existing DHCP Relay Agent Option 82 field.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**NOTE:** The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands [ip dhcp-relay agent-option](#) and [ip dhcp-relay information policy](#) have been configured.

**Syntax** `ip dhcp-relay information policy {append|drop|keep|replace}`  
`no ip dhcp-relay information policy`

| Parameter | Description                                                                                                                                                    |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| append    | The DHCP Relay Agent appends the DHCP Relay Agent Option 82 field of the packet with its own DHCP Relay Agent Option 82 details.                               |
| drop      | The DHCP Relay Agent discards the packet.                                                                                                                      |
| keep      | The DHCP Relay Agent forwards the packet without altering the DHCP Relay Agent Option 82 field.                                                                |
| replace   | The DHCP Relay Agent replaces the existing DHCP Relay Agent details in the DHCP Relay Agent Option 82 field with its own details before forwarding the packet. |

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Examples** To make the DHCP Relay Agent listening on eth0 drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay information policy
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [service dhcp-server](#)

# ip dhcp-relay maxhops

**Overview** This command sets the hop count threshold for discarding BOOTP messages. When the hops field in a BOOTP message exceeds the threshold, the DHCP Relay Agent discards the BOOTP message. The hop count threshold is set to 10 hops by default.

Use the **no** variant of this command to reset the hop count to the default.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay maxhops <1-255>`  
`no ip dhcp-relay maxhops`

| Parameter | Description                  |
|-----------|------------------------------|
| <1-255>   | The maximum hop count value. |

**Default** The default hop count threshold is 10 hops.

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Example** To set the maximum number of hops to 5 for packets received on interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay maxhops 5
```

**Related commands** [service dhcp-relay](#)

# ip dhcp-relay max-message-length

**Overview** This command applies when the device is acting as a DHCP Relay Agent and DHCP Relay Agent Option 82 insertion is enabled. It sets the maximum DHCP message length (in bytes) for the DHCP packet with its DHCP Relay Agent Option 82 data inserted. From this value it calculates the maximum packet size that it will accept at its input. Packets that arrive greater than this value will be dropped.

The **no** variant of this command sets the maximum message length to its default of 1400 bytes.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay max-message-length <548-1472>`  
`no ip dhcp-relay max-message-length`

| Parameter  | Description                                                                                                 |
|------------|-------------------------------------------------------------------------------------------------------------|
| <548-1472> | The maximum DHCP message length (this is the message header plus the inserted DHCP option fields in bytes). |

**Default** The default is 1400 bytes.

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** When a DHCP Relay Agent (that has DHCP Relay Agent Option 82 insertion enabled) receives a request packet from a DHCP client, it will append the DHCP Relay Agent Option 82 component data, and forward the packet to the DHCP server. The DHCP client will sometimes issue packets containing pad option fields that can be overwritten with Option 82 data.

Where there are insufficient pad option fields to contain all the DHCP Relay Agent Option 82 data, the DHCP Relay Agent will increase the packet size to accommodate the DHCP Relay Agent Option 82 data. If the new (increased) packet size exceeds that defined by the **maximum-message-length** parameter, then the DHCP Relay Agent will drop the packet.

**NOTE:** Before setting this command, you must first run the [ip dhcp-relay agent-option](#) command. This will allow the DHCP Relay Agent Option 82 fields to be appended.

**Example** To set the maximum DHCP message length to 1200 bytes for packets arriving in interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay max-message-length 1200
```

To reset the maximum DHCP message length to the default of 1400 bytes for packets arriving in interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay max-message-length
```

**Related commands** [service dhcp-relay](#)



# ip dhcp-relay server-address

**Overview** This command adds a DHCP server for the DHCP Relay Agent to forward client DHCP packets to on a particular interface. You can add up to five DHCP servers on each device interface that the DHCP Relay Agent is listening on.

The **no** variant of this command deletes the specified DHCP server from the list of servers available to the DHCP relay agent.

The **no ip dhcp-relay** command removes all DHCP relay settings from the interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the [DHCP Feature Overview and Configuration Guide](#).

**Syntax** `ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>  
<server-interface>}`  
`no ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>  
<server-interface>}`  
`no ip dhcp-relay`

| Parameter          | Description                                                                                                                                                                   |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv4-address>     | Specify the IPv4 address of the DHCP server for the DHCP Relay Agent to forward client DHCP packets to, in dotted decimal notation. The IPv4 address uses the format A.B.C.D. |
| <ipv6-address>     | Specify the IPv6 address of the DHCPv6 server for the DHCPv6 Relay Agent to forward client DHCP packets to, in hexadecimal notation.                                          |
| <server-interface> | Specify the interface name of the DHCPv6 server. It is only required for a DHCPv6 server with an IPv6 address.                                                                |

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** For a DHCP server with an IPv6 address you must specify the interface for the DHCP server. See examples below for configuration differences between IPv4 and IPv6 DHCP relay servers.

See also the [service dhcp-relay](#) command to enable the DHCP Relay Agent on your device. The [ip dhcp-relay server-address](#) command defines a relay destination on an interface on the device, needed by the DHCP Relay Agent to relay DHCP client packets to a DHCP server.

**Examples: DHCP for IPv4** To enable the DHCP Relay Agent to relay DHCP packets on interface eth0 to the DHCP server with the IPv4 address 192.0.2.200, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-relay server-address 192.0.2.200
```

To remove the DHCP server with the IPv4 address 192.0.2.200 from the list of servers available to the DHCP Relay Agent on interface eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay server-address 192.0.2.200
```

**Examples: DHCPv6** To enable the DHCP Relay Agent on your device to relay DHCP packets on interface eth1.2 to the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface eth1.4, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface eth1.2
awplus(config-if)# ip dhcp-relay server-address
2001:0db8:010d::1 eth1.4
```

To remove the DHCP server with the IPv6 address 2001:0db8:010d::1 on interface eth1.4 from the list of servers available to the DHCP Relay Agent on interface eth1.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1.2
awplus(config-if)# no ip dhcp-relay server-address
2001:0db8:010d::1 eth1.4
```

**Example: disabling DHCP relay** To disable DHCP relay on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-relay
```

**Related commands** [service dhcp-relay](#)

# ip dhcp-relay short-lease-ipv6

**Overview** Use this command to reduce the amount of time an IPv6 address is assigned to a client device.

Long lease times can cause issues in dynamic networks where client devices frequently move between segments, such as VLANs. These device may retain an outdated IP address from its previous VLAN, disrupting communication.

This command is particularly useful in networks with a high turnover of devices or in environments where IP addresses are scarce.

Use the **no** variant of this command to remove the short lease time configuration.

**Syntax** `ip dhcp-relay short-lease-ipv6 [<20-3600> <20-3600>]`  
`no ip dhcp-relay short-lease-ipv6`

| Parameter | Description                                              |
|-----------|----------------------------------------------------------|
| <20-3600> | The valid lease time for IPv6 DHCP relay in seconds.     |
| <20-3600> | The preferred lease time for IPv6 DHCP relay in seconds. |

**Default** Not set

**Mode** Interface Configuration

**Usage notes** The preferred lease time (the second parameter) must be less than the valid lease time (the first parameter).

- **Preferred lease time:** Indicates when preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.
- **Valid lease time:** Indicates when IPv6 addresses or prefixes must be abandoned. An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires.

**Example** To configure a DHCP Relay on interface vlan1 with a valid lease time of 2000 seconds, and a preferred lease time of 1000 seconds for IPv6, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay short-lease-ipv6 2000 1000
```

**Related commands** [show ip dhcp-relay](#)

**Command changes** Version 5.5.4-2.1: command added

## ipv6 address (DHCPv6 PD)

**Overview** Use this command to append an IPv6 address suffix to the IPv6 prefix provided by a DHCPv6 Prefix Delegation (PD) server.

Use the **no** variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

**Syntax** `ipv6 address [<ipv6-prefix-name>] <ipv6-addr/prefix-length> [eui64]`  
`no ipv6 address [<ipv6-prefix-name>] <ipv6-addr/prefix-length> [eui64]`

| Parameter                                    | Description                                                                                                                                                                                 |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-prefix-name&gt;</code>        | The IPv6 prefix name advertised on the router advertisement message sent from the device. The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation. |
| <code>&lt;ipv6-addr/prefix-length&gt;</code> | Specifies the IPv6 address to be set, for example ::1/64. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.                       |
| <code>eui64</code>                           | EUI-64 is a method of automatically deriving the lower 64 bits of an IPv6 address, based on the switch's MAC address.                                                                       |

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** When specifying the **eui64** parameter, the interface identifier of the IPv6 address is derived from the MAC address of the device.

For more information about EUI64, see the [IPv6 Feature Overview and Configuration Guide](#).

**Examples** To assign the IPv6 address 2001:0db8::a2/48 to the interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 address 2001:0db8::a2/48
```

To remove the IPv6 address 2001:0db8::a2/48 from the interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 address 2001:0db8::a2/48
```

To assign the **eui64** derived address in the prefix 2001:0db8::/64 to interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 address 2001:0db8::/64 eui64
```

To remove the **eui64** derived address in the prefix 2001:0db8::/64 from interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 address 2001:0db8::/64 eui64
```

To configure a PD prefix named 'prefix1' on interface eth0 and then add an IPv6 address, use the following commands. In this example, the prefix will be assigned from the pool on the PD client. The host portion or suffix will be ::1 for the last 64 bits:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd prefix1
awplus(config-if)# ipv6 address prefix1::1/64
```

**Related  
commands**

- [ipv6 dhcp client pd](#)
- [ipv6 dhcp pool](#)
- [ipv6 local pool](#)
- [ipv6 nd prefix \(DHCPv6\)](#)
- [prefix-delegation pool](#)
- [show ipv6 dhcp binding](#)
- [show ipv6 interface](#)
- [show ipv6 route](#)
- [show running-config](#)

# ipv6 address dhcp

**Overview** Use this command to activate the DHCPv6 client on the interface that you are configuring. This allows the interface to use the DHCPv6 client to obtain its IPv6 configuration details from a DHCPv6 server on its connected network.

The command also enables IPv6 on the interface, which creates an EUI-64 link-local address as well as enabling RA processing and SLAAC.

Use the **no** variant of this command to stop the interface from obtaining IPv6 configuration details from a DHCPv6 server.

The DHCPv6 client supports the following IP configuration options:

- Option 1—the subnet mask for your device.
- Option 3—a list of default routers.
- Option 6—a list of DNS servers. This list appends the DNS servers set on your device with the [dns-server \(DHCPv6\)](#) command.
- Option 15—a domain name used to resolve host names. This option replaces any domain name that you have set with the [domain-name \(DHCPv6\)](#) command.
- Option 51—lease expiration time.

**Syntax** `ipv6 address dhcp [default-route-to-server]`  
`no ipv6 address dhcp`

| Parameter                            | Description                                                                                                                                                       |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>default-route-to-server</code> | Allow the automatic configuration of a default route to the DHCPv6 server. This option is not enabled by default when you enable the DHCP client on an interface. |

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** Use the **default-route-to-server** option to allow the automatic configuration of a default route to the DHCPv6 server. Note that this option is not enabled by default when you enable the DHCP client on an interface.

**Examples** To set the interface eth0 to use DHCPv6 to obtain an IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 address dhcp
```

To stop the interface eth0 from using DHCPv6 to obtain its IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 address dhcp
```

**Related  
commands**

[clear ipv6 dhcp client](#)  
[ipv6 address](#)  
[ipv6 address \(DHCPv6 PD\)](#)  
[show ipv6 dhcp interface](#)  
[show running-config](#)

# ipv6 dhcp client pd

**Overview** Use this command in Interface Configuration mode to enable the DHCPv6 client process and enable requests for prefix delegation through the interface that you are configuring.

Use the **no** variant of this command to disable requests for prefix delegation. This is the default setting.

For further information about DHCPv6 Prefix Delegation, which is used to automate the process of assigning prefixes, see the [DHCPv6 Feature Overview and Configuration Guide](#).

**Syntax** `ipv6 dhcp client pd <prefix-name> <default-route-to-server>`  
`no ipv6 dhcp client pd`

| Parameter                                    | Description                                                                                                                                                   |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;prefix-name&gt;</code>             | Specify an IPv6 general prefix name. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks". |
| <code>&lt;default-route-to-server&gt;</code> | Specify the default route to the DHCP server                                                                                                                  |

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Default** Prefix delegation is disabled by default on an interface.

**Usage notes** Entering the **ipv6 dhcp client pd** command starts the DHCPv6 client process if not already running, and enables requests for prefix delegation through the interface on which the command is configured.

When prefix delegation is enabled and a prefix is acquired, the prefix is stored in the IPv6 prefix pool with an internal name defined by the required `<prefix-name>` placeholder parameter. The [ipv6 address](#) command can then refer to the prefixes stored in the IPv6 prefix pool.

**Examples** To enable prefix delegation with the prefix name my-prefix-name on the interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd my-prefix-name
```

To disable prefix delegation on the interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 dhcp client pd
```



**Related commands**

- ipv6 enable
- clear ipv6 dhcp client
- ipv6 address (DHCPv6 PD)
- ipv6 nd prefix (DHCPv6)
- show ipv6 dhcp binding
- show ipv6 dhcp interface

# ipv6 dhcp option

**Overview** Use this command in Global Configuration mode to create a user-defined DHCPv6 option. You can then use this option when configuring a DHCPv6 server address pool, by using the [option \(DHCPv6\)](#) command.

Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

Use the **no** variant of this command to remove either the specified user-defined option. This also removes user-defined options from the associated DHCPv6 server address pools.

**Syntax** `ipv6 dhcp option <1-254> [name <option-name>] [<option-type>]`  
`no ipv6 dhcp option <1-254>|<option-name>`

| Parameter     | Description                                                                                                                                                                                                                          |                                                                                                                                                                                                                                |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-254>       | The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.                                                                                               |                                                                                                                                                                                                                                |
| <option-name> | Option name used to identify the option. You cannot use a number as the option name. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".<br>Default: no default |                                                                                                                                                                                                                                |
| <option-type> | The option value. You must specify a value that is appropriate to the option type:                                                                                                                                                   |                                                                                                                                                                                                                                |
|               | ascii                                                                                                                                                                                                                                | An ASCII text string                                                                                                                                                                                                           |
|               | hex                                                                                                                                                                                                                                  | A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.                                    |
|               | ipv6                                                                                                                                                                                                                                 | An IPv6 address or prefix that has hexadecimal notation in the format HHHH : HHHH : : HHHH : HHHH. To create a list of IPv6 addresses, you must add each IPv6 address individually by using the option command multiple times. |
|               | integer                                                                                                                                                                                                                              | A number from 0 to 4294967295.                                                                                                                                                                                                 |
|               | flag                                                                                                                                                                                                                                 | A value that either sets (to 1) or unsets (to 0) a flag: <b>true</b> , <b>on</b> , or <b>enabled</b> will set the flag. <b>false</b> , <b>off</b> or <b>disabled</b> will unset the flag.                                      |

**Mode** Global Configuration

**Examples** To define a user-defined ASCII string option as option 66, without a name, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 66 ascii
```

To define a user-defined hexadecimal string option as option 46, with the name "tcpip-node-type", use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 46 name tcpip-node-type hex
```

To define a user-defined IP address option as option 175, with the name special-address, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 175 name special-address ip
```

To remove the specific user-defined option with the option number 12, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp option 12
```

To remove the specific user-defined option with the option name perform-router-discovery, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp option perform-router-discovery
```

**Related commands**

- [dns-server \(DHCPv6\)](#)
- [domain-name \(DHCPv6\)](#)
- [option \(DHCPv6\)](#)
- [show ipv6 dhcp](#)

# ipv6 dhcp pool

**Overview** Use this command in Global Configuration mode to enter the DHCPv6 Configuration mode for the DHCPv6 server pool name as specified in the required command parameter. If the name specified is not associated with an existing pool, the device will create a new pool with this name, then enter the configuration mode for the new pool.

Once you have entered the DHCPv6 configuration mode, all commands executed before the next **exit** command will apply to this pool.

You can create multiple DHCPv6 server pools on devices with multiple interfaces. This allows the device to act as a DHCPv6 server on multiple interfaces to distribute different information to clients on the different networks.

Use the **no** variant of this command to delete the specific DHCPv6 pool.

**Syntax** `ipv6 dhcp pool <DHCPv6-poolname>`  
`no ipv6 dhcp pool <DHCPv6-poolname>`

| Parameter                            | Description                                                                                                                                                                    |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;DHCPv6-poolname&gt;</code> | Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks". |

**Mode** Global Configuration

**Usage** All DHCPv6 prefix pool names must be unique. IPv6 prefix pools have a similar function to IPv4 address pools. Contrary to IPv4, a block of IPv6 addresses (an IPv6 address prefix) are assigned and not single IPv6 addresses. IPv6 prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, you must remove then recreate a IPv6 prefix pool. All IPv6 prefixes already allocated are also freed.

**Examples** To create the DHCPv6 pool named P2 and enter DHCPv6 configuration mode, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)#
```

To delete the DHCPv6 pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp pool P2
```

**Related  
commands**

- ipv6 local pool
- option (DHCPv6)
- prefix-delegation pool
- show ipv6 dhcp binding
- show ipv6 dhcp pool

# ipv6 dhcp server

**Overview** Use this command in Interface Configuration mode to enable DHCPv6 server for the current IPv6 configured interface to use the specified DHCPv6 server pool name.

The DHCPv6 server service listens for DHCPv6 requests on the IPv6 configured interface. The DHCPv6 server service does not run on interfaces without IPv6 configured on them.

Use the **no** variant of this command to disable the DHCPv6 server.

**Syntax** `ipv6 dhcp-server [<DHCPv6-poolname>]`  
`no ipv6 dhcp-server`

| Parameter         | Description                                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <DHCPv6-poolname> | Specify a named DHCPv6 server pool as defined with the <a href="#">ipv6 dhcp pool</a> command. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks". |

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** The **ipv6 dhcp server** command enables the DHCPv6 service on a specified interface using the pool for prefix delegation and configuration through the specified interface.

Note that DHCPv6 client, DHCPv6 server and DHCPv6 relay are mutually exclusive on an interface. When one of the DHCPv6 functions is enabled on an interface then another DHCPv6 function cannot be enabled on the same interface.

**Examples** To enable the DHCPv6 server service and use the DHCPv6 pool named P2 on interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 dhcp server P2
```

To disable the DHCPv6 server on interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 dhcp server
```

**Related commands** [ipv6 dhcp pool](#)  
[show ipv6 dhcp binding](#)  
[show ipv6 dhcp pool](#)

# ipv6 local pool

**Overview** Use this command in Global Configuration mode to configure a local DHCPv6 server prefix delegation pool specifying a poolname and a prefix/prefix length. You can optionally exclude the locally assigned prefix from the pool with the **exclude-local-prefix** keyword.

Use the **no** variant of this command to remove a local DHCPv6 server prefix delegation pool specifying the poolname.

**Syntax** `ipv6 local pool <DHCPv6-poolname> <delegated-prefix-name>  
<ipv6-prefix/prefix-length> <assigned-length>  
[exclude-local-prefix]`  
`no ipv6 local pool`

| Parameter                                      | Description                                                                                                                                                                                                                                                                                          |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;DHCPv6-poolname&gt;</code>           | Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".                                                                                                                       |
| <code>&lt;delegated-prefix-name&gt;</code>     | Description used to identify the delegated prefix name from the parent PD (Prefix Delegation) server. If the name contains spaces then you must enclose it in "quotation marks".                                                                                                                     |
| <code>&lt;ipv6-prefix/prefix-length&gt;</code> | Specify an IPv6 prefix and prefix length. The prefix length indicates the length of the IPv6 prefix assigned to the pool.<br>The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.                                                             |
| <code>&lt;assigned-length&gt;</code>           | Specify an IPv6 prefix length assigned to the user from the pool in the range <1-128>. Note that the value of the <i>assigned-length</i> parameter entered cannot be less than or equal to the <i>prefix-length</i> parameter value entered. An assigned length must be longer than a prefix length. |
| <code>exclude-local-prefix</code>              | Specify this keyword to exclude the locally assigned prefix from the pool.                                                                                                                                                                                                                           |

**Default** No DHCPv6 server prefix delegation pool is configured by default.

**Mode** Global Configuration

**Usage notes** All IPv6 prefix pool names must be unique. IPv6 prefix pools have a similar function to IPv4 address pools. Contrary to IPv4, a block of IPv6 addresses (an IPv6 address prefix) are assigned and not single IPv6 addresses. IPv6 prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, you must remove then recreate a IPv6 prefix pool. All IPv6 prefixes already allocated are also freed.

**Examples** To create a local DHCPv6 local pool named P2 with the IPv6 prefix and prefix length 2001:0db8::/32 with an assigned length of 64, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 local pool P2 2001:0db8::/32 64
```

To remove a configured DHCPv6 local pool, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 local pool
```

**Related commands** [ipv6 dhcp pool](#)  
[show ipv6 dhcp pool](#)



## ipv6 nd prefix (DHCPv6)

**Overview** Use this command to specify IPv6 RA (Router Advertisement) prefix information generated from the DHCPv6 server for DHCPv6 prefix-delegation for an interface.

Use the **no** variant of this command to remove IPv6 RA prefix information from the DHCPv6 Server for DHCPv6 Prefix-Delegation for the interface. Use the **all** parameter with the **no** variant of this command to remove all prefix names and all prefixes for an interface.

**Syntax** `ipv6 nd prefix <ipv6-prefix-name>  
<ipv6-prefix/length>{<valid-lifetime>|infinite}  
{<preferred-lifetime>|infinite} {off-link|no-autoconfig}`  
`no ipv6 nd prefix {<ipv6-prefix-name>|<ipv6-prefix/length>|all}`

| Parameter                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-prefix-name&gt;</code>   | The IPv6 prefix name advertised on the router advertisement message sent from the device.<br>The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation.                                                                                                                                                                                                                                         |
| <code>&lt;ipv6-prefix/length&gt;</code> | The IPv6 prefix and prefix length advertised on the router advertisement message sent from the device.<br>The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.                                                                                                                                                                                                              |
| <code>&lt;valid-lifetime&gt;</code>     | The the period during which the specified IPv6 address prefix is valid. This can be set to a value between 5 and 315360000 seconds. Note that this period should be set to a value greater than that set for the prefix preferred-lifetime. See the Usage notes after this parameter table for a description of valid lifetime and how it determines invalid IPv6 addresses upon expiry.                                               |
| <code>infinite</code>                   | Specifying this keyword instead of entering a value for the <code>&lt;valid-lifetime&gt;</code> parameter applies an infinite valid lifetime.                                                                                                                                                                                                                                                                                          |
| <code>&lt;preferred-lifetime&gt;</code> | Specifies the IPv6 prefix preferred lifetime. This is the period during which the IPv6 address prefix is considered current. Set this to a value between 0 and 315360000 seconds. Note that this period should be set to a value less than that set for the prefix valid-lifetime. See the Usage notes after this parameter table for a description of preferred lifetime and how it determines deprecated IPv6 addresses upon expiry. |
| <code>infinite</code>                   | Specifying this keyword instead of entering a value for the <code>&lt;preferred-lifetime&gt;</code> parameter applies an infinite valid lifetime.                                                                                                                                                                                                                                                                                      |
| <code>off-link</code>                   | Specify the IPv6 prefix off-link flag.                                                                                                                                                                                                                                                                                                                                                                                                 |
| <code>no-autoconfig</code>              | Specify the IPv6 prefix no autoconfiguration flag. Setting this flag indicates that the prefix is not to be used for autoconfiguration.                                                                                                                                                                                                                                                                                                |
| <code>all</code>                        | Specify all prefix names and all prefixes are removed when used with the no variant of this command.                                                                                                                                                                                                                                                                                                                                   |

**Mode** Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

**Usage notes** This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Examples** The following example configures the device to issue RAs (Router Advertisements) on the interface eth0, and advertises the DHCPv6 prefix name prefix1 and the IPv6 address prefix of 2001:0db8::/32.

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd prefix1
awplus(config-if)# ipv6 nd prefix prefix1 2001:0db8::/32
```

The following example resets router advertisements on the interface eth0, so the address prefix of 2001:0db8::/32 is not advertised from the device.

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/32
```

The following example removes all prefix names and prefixes from interface eth0:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd prefix all
```

**Related commands**

- [ipv6 address \(DHCPv6 PD\)](#)
- [ipv6 dhcp client pd](#)
- [ipv6 dhcp pool](#)
- [ipv6 local pool](#)
- [prefix-delegation pool](#)
- [show ipv6 dhcp binding](#)

# link-address

**Overview** Use this command in DHCPv6 Configuration mode to specify a link-address prefix within a DHCPv6 Server pool.

Note that you can only configure one link address per DHCPv6 pool. Configuring another link address in the same DHCPv6 pool overwrites the previously configured link address.

Use the **no** variant of this command to remove the link-address prefix from the DHCPv6 Server pool.

**Syntax** `link-address <ipv6-prefix/prefix-length>`  
`no link-address`

| Parameter                                      | Description                                                                                                                                                                                                                           |
|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-prefix/prefix-length&gt;</code> | Specify an IPv6 prefix and prefix length. The prefix length indicates the length of the IPv6 prefix assigned to the pool. The IPv6 address uses the format X:X::X/X/Prefix-Length. The prefix-length is usually set between 0 and 64. |

**Default** No DHCPv6 Server pool configuration link address prefix is configured by default.

**Mode** DHCPv6 Configuration

**Usage notes** Link addresses are configured in DHCPv6 Server address pools when there are remote clients that communicate via intermediate relay(s).

RELAY-FORW and RELAY-REPL relay packets contain the requesting link address source.

This command is used to match incoming requests from PD (Prefix Delegation) clients (received via an intermediate relay) to a configured delegation pool.

When an address on the incoming interface of the DHCPv6 server or a link address set in the incoming delegation request packet from the prefix delegation client matches the link-address prefix configured in the delegation pool, the DHCPv6 server is able to match and use the appropriate delegation pool for relayed delegation request messages.

If there is no match between incoming delegation request packets from the prefix delegation client and the link-address prefix configured in the delegation pool, the DHCPv6 Server does not delegate an IPv6 prefix to the requesting device.

The link address should be set to the network prefix where the prefix delegation client resides. The prefix delegation server will also need a forwarding path (IPv6 route) back to the network prefix where the prefix delegation client resides.

For more information, see the [DHCPv6 Feature Overview and Configuration Guide](#).

**Examples** To configure the IPv6 prefix and prefix length 2001:0db8:1::/48 as the link address for pool P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# address prefix 2001:0db8:2::/48
awplus(config-dhcp6)# link-address 2001:0db8:1::/48
```

To remove the link address, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# no link-address
```

**Related commands** [ipv6 dhcp pool](#)  
[show ipv6 dhcp pool](#)

## option (DHCPv6)

**Overview** Use this command in DHCPv6 Configuration mode to add a user-defined option to the DHCPv6 prefix pool you are configuring. For the **hex**, **integer**, and **flag** option types, if the option already exists, the new option overwrites the existing option's value.

Use the **no** variant of this command to remove the specified user-defined option from the DHCPv6 server pool, or to remove all user-defined options from the DHCPv6 server pool.

**Syntax** `option [<1-254>|<option-name>] <option-value>`  
`no option [<1-254>|<option-value>]`

| Parameter      | Description                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-254>        | The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.                                                                 |
| <option-name>  | Option name associated with the option.                                                                                                                                                                |
| <option-value> | The option value. You must specify a value that is appropriate to the option type:                                                                                                                     |
|                | <b>hex</b> A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long. |
|                | <b>ipv6</b> An IPv6 prefix that has the hexadecimal X:X::X:X notation. To create a list of IPv6 prefixes, you must add each IPv6 prefix individually using this command multiple times.                |
|                | <b>integer</b> A number from 0 to 4294967295.                                                                                                                                                          |
|                | <b>flag</b> A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag.                                                                                       |

**Mode** DHCPv6 Configuration

**Usage** You must define a DHCPv6 option using the `ipv6 dhcp option` command before using the `option (DHCPv6)` command.

Note that options with an **ipv6** type can hold a list of IPv6 prefix (i.e. entries that have the X:X::X:X address format), so if the option already exists in the pool, then the new IP address is added to the list of existing IPv6 prefixes. Also note options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

**Examples** To add the IPv6 type option named `sntp-server-addr` to the pool P2 and give the option the value `ipv6`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 22 name sntp_server_addr ipv6
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option sntp_server_addr ipv6
```

To add the ASCII-type option named `tftp-server-name` to the pool P2 and give the option the value `server1`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option tftp-server-name server1
```

To add the hex-type option named `tcpip-node-type` to the pool P2 and give the option the value `08af`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option tcpip-node-type 08af
```

To add multiple IP addresses for the ip-type option 175, use the following commands:

```
awplus(config-dhcp6)# option 175 2001:0db8:3001::/64
awplus(config-dhcp6)# option 175 2001:0db8:3002::/64
awplus(config-dhcp6)# option 175 2001:0db8:3003::/64
```

To add the option 179 to a pool, and give the option the value 123456, use the following command:

```
awplus(config-dhcp6)# option 179 123456
```

To add a user-defined flag option with the name `perform-router-discovery`, use the following command:

```
awplus(config-dhcp6)# option perform-router-discovery yes
```

To clear all user-defined options from a DHCP address pool, use the following command:

```
awplus(config-dhcp6)# no option
```

To clear a user-defined option, named `tftp-server-name`, use the following command:

```
awplus(config-dhcp6)# no option tftp-server-name
```

**Related commands**

- [dns-server \(DHCPv6\)](#)
- [ipv6 dhcp option](#)
- [ipv6 dhcp pool](#)
- [show ipv6 dhcp pool](#)

# prefix-delegation pool

**Overview** Use this command in DHCPv6 Configuration mode to add a DHCPv6 server prefix-delegation pool entry to the current DHCPv6 pool configuration. You must define a DHCPv6 server prefix-delegation pool using the [ipv6 dhcp pool](#) command before using this command.

Use the **no** variant of this command to remove a DHCPv6 server prefix-delegation pool from the current DHCPv6 pool configuration.

**Syntax** `prefix-delegation pool <DHCPv6-poolname> [lifetime {<valid-time>|infinite} {<preferred-time>|infinite}]`  
`no prefix-delegation pool <DHCPv6-poolname>`

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <DHCPv6-poolname> | Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".                                                                                                                                                                                                        |
| lifetime          | Optional. Specify a time period for the hosts to remember router advertisements (RAs). If you specify this parameter then you must also specify a <i>valid-time</i> and a <i>preferred-time</i> value.<br>See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry. |
| <valid-time>      | Specify a valid lifetime in seconds in the range <5-315360000>.                                                                                                                                                                                                                                                                                                                       |
| infinite          | Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.                                                                                                                                                                                                                                                                               |
| <preferred-time>  | Specify a valid lifetime in seconds in the range <5-315360000>.                                                                                                                                                                                                                                                                                                                       |

**Default** No IPv6 local prefix pool is specified by default.

**Mode** DHCPv6 Configuration

**Usage notes** The DHCPv6 server assigns prefixes dynamically from an IPv6 local prefix pool, which is configured using the [ipv6 local pool](#) command and is associated with a DHCPv6 configuration pool using this command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes from the pool. After the client releases the previously assigned prefixes, the server returns the prefixes to the pool for reassignment.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source

address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

**Example** This example adds DHCPv6 Prefix Delegation pool pd\_pool1 to DHCPv6 pool pool1:

```
awplus# configure terminal
awplus(config)# ipv6 local pool pd_pool1 2001:0db8::/48 56
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# prefix-delegation pool pd_pool1
```

**Related commands**

- [ipv6 dhcp pool](#)
- [ipv6 local pool](#)
- [show ipv6 dhcp pool](#)



# service dhcp-relay

**Overview** This command enables the DHCP Relay Agent on the device. However, on a given IP interface, no DHCP forwarding takes place until at least one DHCP server is specified to forward/relay all clients' DHCP packets to.

The **no** variant of this command disables the DHCP Relay Agent on the device for all interfaces.

**Syntax** `service dhcp-relay`  
`no service dhcp-relay`

**Mode** Global Configuration

**Usage notes** A maximum number of 400 DHCP Relay Agents (one per interface) can be configured on the device. Once this limit has been reached, any further attempts to configure DHCP Relay Agents will not be successful.

**Default** The DHCP-relay service is enabled by default.

**Examples** To enable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
```

To disable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# no service dhcp-relay
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [ip dhcp-relay information policy](#)
- [ip dhcp-relay maxhops](#)
- [ip dhcp-relay server-address](#)

# show counter dhcp-relay

**Overview** This command shows counters for the DHCP Relay Agent on your device.  
For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show counter dhcp-relay

**Mode** User Exec and Privileged Exec

**Examples** To display counters for the DHCP Relay Agent on your device, use the following command:

```
awplus# show counter dhcp-relay
```

**Output** Figure 46-2: Example output from the **show counter dhcp-relay** command

```
awplus#show counter dhcp-relay

DHCP relay counters
Requests In 4
Replies In 4
Relayed To Server 4
Relayed To Client 4
Out To Server Failed 0
Out To Client Failed 0
Invalid hlen 0
Bogus giaddr 0
Corrupt Agent Option 0
Missing Agent Option 0
Bad Circuit ID 0
Missing Circuit ID 0
Bad Remote ID 0
Missing Remote ID 0
Option Insert Failed 0
DHCPv6 Requests In 0
DHCPv6 Replies In 0
DHCPv6 Relayed to Server 0
DHCPv6 Relayed to Client 0
```

| Parameter         | Description                                                |
|-------------------|------------------------------------------------------------|
| Requests In       | The number of DHCP Request messages received from clients. |
| Replies In        | The number of DHCP Reply messages received from servers.   |
| Relayed To Server | The number of DHCP Request messages relayed to servers.    |
| Relayed To Client | The number of DHCP Reply messages relayed to clients.      |

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Out To Server Failed | The number of failures when attempting to send request messages to servers. This is an internal debugging counter.                                                                                                                                                                                                                                                                                                                                                                 |
| Out To Client Failed | The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.                                                                                                                                                                                                                                                                                                                                                                   |
| Invalid hlen         | The number of incoming messages dropped due to an invalid hlen field.                                                                                                                                                                                                                                                                                                                                                                                                              |
| Bogus giaddr         | The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.                                                                                                                                                                                                                                                                                                                                                                                                  |
| Corrupt Agent Option | The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command. |
| Missing Agent Option | The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command. |
| Bad Circuit ID       | The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.                               |
| Missing Circuit ID   | The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command.                           |

| Parameter                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Bad Remote ID            | The number of incoming DHCP Reply messages dropped due to a bad remote ID.<br>Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command                                                                                                                                                |
| Missing Remote ID        | The number of incoming DHCP Reply messages dropped due to a missing remote ID.<br>Note that Agent Option counters only increment on errors occurring if the <code>ip dhcp-relay agent-option</code> command is configured for an interface. Messages generating the errors are only dropped if the <code>ip dhcp-relay agent-option checking</code> command is configured on the interface as well as the <code>ip dhcp-relay agent-option</code> command                                                                                                                                            |
| Option Insert Failed     | The number of incoming DHCP Request messages dropped due to an error adding the DHCP Relay Agent information (option-82). This counter increments when: <ul style="list-style-type: none"> <li>the DHCP Relay Agent is set to drop packets with the DHCP Relay Agent Option 82 field already filled by another DHCP Relay Agent. This policy is set with the <code>ip dhcp-relay information policy</code> command.</li> <li>there is a packet error that stops the DHCP Relay Agent from being able to append the packet with its DHCP Relay Agent Information Option (Option 82) field.</li> </ul> |
| DHCPv6 Requests In       | The number of incoming DHCPv6 Request messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| DHCPv6 Replies In        | The number of incoming DHCPv6 Reply messages.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| DHCPv6 Relayed to Server | The number of DHCPv6 messages relayed to the server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| DHCPv6 Relayed to Client | The number of DHCPv6 messages relayed to the client.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |

# show counter ipv6 dhcp-client

**Overview** Use this command in User Exec or Privilege Exec mode to show DHCPv6 client counter information. See [show counter ipv6 dhcp-server](#) for DHCPv6 server information.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show counter ipv6 dhcp-client`

**Mode** User Exec and Privileged Exec

**Example** To display the DHCPv6 client counter information, use the command:

```
awplus# show counter ipv6 dhcp-client
```

**Output** Figure 46-3: Example output from the **show counter ipv6 dhcp-client** command

```
awplus#show counter ipv6 dhcp-client
SOLICIT out 20
ADVERTISE in 12
REQUEST out 1
CONFIRM out 0
RENEW out 0
REBIND out 0
REPLY in 0
RELEASE out 0
DECLINE out 0
INFORMATION-REQUEST out 0
```

**Table 1:** Parameters in the output of the **show counter ipv6 dhcp-client** command

| Parameter    | Description                                                             |
|--------------|-------------------------------------------------------------------------|
| SOLICIT out  | Displays the count of SOLICIT messages sent by the DHCPv6 client.       |
| ADVERTISE in | Displays the count of ADVERTISE messages received by the DHCPv6 client. |
| REQUEST out  | Displays the count of REQUEST messages sent by the DHCPv6 client.       |
| CONFIRM out  | Displays the count of CONFIRM messages sent by the DHCPv6 client.       |
| RENEW out    | Displays the count of RENEW messages sent by the DHCPv6 client.         |

**Table 1:** Parameters in the output of the **show counter ipv6 dhcp-client** command (cont.)

| Parameter               | Description                                                                   |
|-------------------------|-------------------------------------------------------------------------------|
| REBIND out              | Displays the count of REBIND messages sent by the DHCPv6 client.              |
| REPLY in                | Displays the count of REPLY messages received by the DHCPv6 client.           |
| RELEASE out             | Displays the count of RELEASE messages sent by the DHCPv6 client.             |
| DECLINE out             | Displays the count of DECLINE messages sent by the DHCPv6 client.             |
| INFORMATION-REQUEST out | Displays the count of INFORMATION-REQUEST messages sent by the DHCPv6 client. |

**Related commands** [show counter ipv6 dhcp-server](#)

# show counter ipv6 dhcp-server

**Overview** Use this command in User Exec or Privileged Exec mode to show DHCPv6 server counter information. See [show counter ipv6 dhcp-client](#) for DHCPv6 client information.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show counter ipv6 dhcp-server

**Mode** User Exec and Privileged Exec

**Example** To display the DHCPv6 server counter information, use the command:

```
awplus# show counter ipv6 dhcp-server
```

**Output** Figure 46-4: Example output from the **show counter ipv6 dhcp-server** command

```
awplus#show counter ipv6 dhcp-server
SOLICIT in 20
ADVERTISE out 12
REQUEST in 1
CONFIRM in 0
RENEW in 0
REBIND in 0
REPLY out 0
RELEASE in 0
DECLINE in 0
INFORMATION-REQUEST in 0
RELAY FORWARD in 0
LEASEQUERY in 0
DHCPv4 QUERY in 0
```

**Table 2:** Parameters in the output of the **show counter ipv6 dhcp-server** command

| Parameter     | Description                                                           |
|---------------|-----------------------------------------------------------------------|
| SOLICIT in    | Displays the count of SOLICIT messages received by the DHCPv6 server. |
| ADVERTISE out | Displays the count of ADVERTISE messages sent by the DHCPv6 server.   |
| REQUEST in    | Displays the count of REQUEST messages received by the DHCPv6 server. |
| CONFIRM in    | Displays the count of CONFIRM messages received by the DHCPv6 server. |

**Table 2:** Parameters in the output of the **show counter ipv6 dhcp-server** command (cont.)

| Parameter              | Description                                                                      |
|------------------------|----------------------------------------------------------------------------------|
| RENEW in               | Displays the count of RENEW messages received by the DHCPv6 server.              |
| REBIND in              | Displays the count of REBIND messages received by the DHCPv6 server.             |
| REPLY out              | Displays the count of REPLY messages sent by the DHCPv6 server.                  |
| RELEASE in             | Displays the count of RELEASE messages received by the DHCPv6 server.            |
| DECLINE in             | Displays the count of DECLINE messages received by the DHCPv6 server.            |
| INFORMATION-REQUEST in | Displays the count of INFORMATION-REQUEST messages received by the DHCPv6 server |
| RELAY FORWARD in       | Displays the count of Relay forward in messages received by the DHCPv6 server    |
| LEASEQUERY in          | Displays the count of LEASE QUERY messages received by the DHCPv6 server         |
| DHCPv4 QUERY in        | Displays the count of DHCPv4 QUERY messages received by the DHCPv6 server        |

**Related commands** [show counter ipv6 dhcp-client](#)



# show ip dhcp-relay

**Overview** This command shows the configuration of the DHCP Relay Agent on each interface.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ip dhcp-relay [interface <interface-name>]`

| Parameter        | Description                                                                                          |
|------------------|------------------------------------------------------------------------------------------------------|
| <interface-name> | Name of a specific interface. This displays the DHCP configuration for the specified interface only. |

**Mode** User Exec and Privileged Exec

**Example** To display the DHCP Relay Agent’s configuration on the interface eth0, use the command:

```
awplus# show ip dhcp-relay interface eth0
```

**Output** Figure 46-5: Example output from the **show ip dhcp-relay** command

```
DHCP Relay Service is enabled

eth0 is up, line protocol is up
Maximum hop count is 10
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
The Remote Id string for Relay Agent Option is 0000.cd28.074c
Relay information policy is to append new relay agent
information
List of servers : 192.168.1.200
```

**Related commands**

- [ip dhcp-relay agent-option](#)
- [ip dhcp-relay agent-option checking](#)
- [ip dhcp-relay information policy](#)
- [ip dhcp-relay maxhops](#)
- [ip dhcp-relay server-address](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# show ipv6 dhcp

**Overview** Use this command in User Exec or Privileged Exec mode to show the DHCPv6 unique identifier (DUID) configured on your device.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 dhcp`

**Mode** User Exec and Privileged Exec

**Usage notes** The DUID is based on the link-layer address for both DHCPv6 client and DHCPv6 server identifiers. The device uses the MAC address from the lowest interface number for the DUID.

The DUID is used by a DHCPv6 client to obtain an IPv6 address from a DHCPv6 server. A DHCPv6 server compares the DUID with its database of DUIDs and sends configuration data for an IPv6 address plus the preferred and valid lease time values to a DHCPv6 client.

**Example** To display the DUID configured on your device, use the command:

```
awplus# show ipv6 dhcp
```

**Output** Figure 46-6: Example output from the **show ipv6 dhcp** command

```
awplus#show ipv6 dhcp
DHCPv6 Server DUID: 0001000117ab6876001577f7ba23
```

**Related commands** [ipv6 address dhcp](#)

# show ipv6 dhcp binding

**Overview** Use this command in User Exec or Privileged Exec mode to show the IPv6 address entries that the DHCPv6 server leases to DHCPv6 clients. Note that applying this command with the optional *summary* keyword parameter displays the number of addresses per pool, but not the address or prefix entries per pool.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 dhcp binding [summary]`

| Parameter            | Description                                                                                                                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>summary</code> | Optional. Specify the <b>summary</b> keyword to display summarized information for DHCPv6 server leases to client nodes, displaying the number of address entries per pool, not the addresses or prefixes. |

**Mode** User Exec and Privileged Exec

**Example 1** To display the total DHCPv6 leasing address entries for all pools, use the command:

```
awplus# show ipv6 dhcp binding summary
```

**Output** Figure 46-7: Example output from the **show ipv6 dhcp binding summary** command

|                                        |                            |
|----------------------------------------|----------------------------|
| awplus# show ipv6 dhcp binding summary |                            |
| Pool Name                              | Number of Leased Addresses |
| -----                                  |                            |
| ia-na1                                 | 3                          |
| ia-pd1                                 | 5                          |
| Total in all Pools:                    | 8                          |

**Table 3:** Parameters in the output of the **show ipv6 dhcp binding summary** command

| Parameter                  | Description                                                        |
|----------------------------|--------------------------------------------------------------------|
| Pool Name                  | Displays a list of all the pool names.                             |
| Number of Leased Addresses | Displays the number of leased address entries for the pool.        |
| Total in all Pools         | Displays the total number of leased address entries for all pools. |

**Example 2** To display addresses, prefixes, and lifetimes for all DHCPv6 leasing entries by pool, enter:

```
awplus# show ipv6 dhcp binding
```

**Output** Figure 46-8: Example output from the **show ipv6 dhcp binding** command

```
awplus#show ipv6 dhcp binding
Pool ia-na1
 Address 2002:0:3c0::1
 client IAID 77f7ba23, DUID 0001000117c4bbb4001577f7ba23
 preferred lifetime 604800, valid lifetime 2592000
 starts at 20 Aug 2012 18:38:29
 expires at 19 Sep 2012 18:38:29
Pool ia-pd1
 Prefix 2002:0:3c0::/42
 client IAID 77f7ba23, DUID 0001000117c4bbb4001577f7ba23
 preferred lifetime 604800, valid lifetime 2592000
 starts at 20 Aug 2012 18:38:29
 expires at 19 Sep 2012 18:38:29
```

**Table 4:** Parameters in the output of the **show ipv6 dhcp binding** command

| Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Address            | Address delegated to the indicated IAID and DUID.<br>See the IAID and DUID descriptions below for further information.                                                                                                                                                                                                                                                                                                                                                                       |
| Prefix             | Prefix delegated to the indicated IAID and DUID.<br>See the IAID and DUID descriptions below for further information.                                                                                                                                                                                                                                                                                                                                                                        |
| DUID               | DHCPv6 unique identifier (DUID) (see RFC 3315).<br>Each DHCPv6 client has as DUID. DHCPv6 servers use DUIDs to identify clients for the association of IAs (Identity Associations) with DHCPv6 clients. DHCPv6 clients use DUIDs to identify a DHCPv6 server.                                                                                                                                                                                                                                |
| IAID               | Identify Association Identifier (IAID) (see RFC 3315).<br>IAIDs are identifiers for IAs (Identity Associations), where an IA is a collection of IPv6 addresses assigned to a DHCPv6 client. Each IA has an associated IAD. Each DHCPv6 client may have more than one IA assigned to it. Each IA holds one type of address.                                                                                                                                                                   |
| preferred lifetime | The preferred lifetime setting in seconds for the specified IAID and DUID. Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires. Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected. |
| valid lifetime     | The valid lifetime setting in seconds for the specified IAID and DUID. An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.                                                                                                                                                                                                      |

**Table 4:** Parameters in the output of the **show ipv6 dhcp binding** command

| Parameter  | Description                                            |
|------------|--------------------------------------------------------|
| starts at  | The date and time at which the valid lifetime expires. |
| expires at | The date and time at which the valid lifetime expires. |

**Related  
commands**

[clear ipv6 dhcp binding](#)

[ipv6 dhcp pool](#)

[show ipv6 dhcp pool](#)

# show ipv6 dhcp interface

**Overview** Use this command in User Exec or Privileged Exec mode to display DHCPv6 information for a specified interface, or all interfaces when entered without the interface parameter.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 dhcp interface [<interface-name>]`

| Parameter        | Description                                                                                                                                                                          |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface-name> | Optional. Specify the name of the interface to show DHCPv6 information about. Omit this optional parameter to display DHCPv6 information for all interfaces DHCPv6 is configured on. |

**Mode** User Exec and Privileged Exec

**Example** To display DHCPv6 information for all interfaces DHCPv6 is configured on, use the command:

```
awplus# show ipv6 dhcp interface
```

To display DHCPv6 information for interface eth0, use the command:

```
awplus# show ipv6 dhcp interface eth0
```

**Output** Figure 46-9: Example output from the **show ipv6 dhcp interface** command

```
awplus# show ipv6 dhcp interface
eth1 is in client mode
 Address 1001::3c0:1
 preferred lifetime 9000, valid lifetime 5000
 starts at 20 Jan 2021 09:21:35
 expires at 20 Jan 2021 10:25:32
```

Figure 46-10: Example output from the **show ipv6 dhcp interface** command for a specific interface

```
awplus# show ipv6 dhcp interface eth0
eth0 is in client (Prefix-Delegation) mode
 Prefix name pd1
 prefix 2002:0:3c0::/42
 preferred lifetime 604800, valid lifetime 2592000
 starts at 20 Aug 2021 09:21:33
 expires at 19 Sep 2021 09:21:33
```

**Table 5:** Parameters in the output of the **show counter dhcp-client** command

| Parameter                                                 | Description                                                                                                                    |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| <interface> is in server/client/ (Prefix-Delegation) mode | Displays whether the specified interface is in server or client mode and whether prefix-delegation is applied to an interface. |
| Address                                                   | Displays the address of the DHCPv6 server on the interface.                                                                    |
| Prefix name                                               | Displays the IPv6 general prefix pool name, where prefixes are stored for the interface.                                       |
| Using pool                                                | Displays the name of the pool used by the interface.                                                                           |
| Preference                                                | Displays the preference value for the DHCPv6 server.                                                                           |

**Related commands**    [ipv6 dhcp client pd](#)

# show ipv6 dhcp pool

**Overview** Use this command in User Exec or Privileged Exec mode to display the configuration details and system usage of the DHCPv6 address pools configured on the device.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** `show ipv6 dhcp pool [<DHCPv6-address-pool-name>]`

| Parameter                  | Description                                                                                                        |
|----------------------------|--------------------------------------------------------------------------------------------------------------------|
| <DHCPv6-address-pool-name> | Name of a specific DHCPv6 address pool. This displays the configuration of the specified DHCPv6 address pool only. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ipv6 dhcp pool`

**Output** Figure 46-11: Example output from the **show ipv6 dhcp pool** command

|                                              |
|----------------------------------------------|
| awplus# show ipv6 dhcp pool                  |
| DHCPv6 Pool: ia-na                           |
| Address Prefix : 1001::/64                   |
| Lifetime: 2592000(valid), 604800(preferred)  |
| DNS Server: 2001::1                          |
| DNS Server: 2001::2                          |
| Domain Name: example.com                     |
| Domain Name: example.co.jp                   |
| SNTP Server: 2001::5                         |
| SNTP Server: 2001::6                         |
| Option Code : 150                            |
| Value: [ASCII] test-test                     |
| DHCPv6 Pool: ia-pd                           |
| PD Pool Name: pd1                            |
| Prefix : 2002::/38-42                        |
| Lifetime : 2592000(valid), 604800(preferred) |

**Table 6:** Parameters in the output of the **show ipv6dhcp pool** command

| Parameter      | Description                        |
|----------------|------------------------------------|
| DHCPv6 Pool    | Name of the DHCPv6 pool.           |
| Address Prefix | Address prefix to the DHCPv6 pool. |



**Table 6:** Parameters in the output of the **show ipv6dhcp pool** command (cont.)

| Parameter           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Address<br>Lifetime | <p>Valid and preferred lifetimes to the DHCPv6 pool.</p> <p>Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.</p> <p>Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.</p> <p>An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.</p> |
| DNS Server          | IPv6 address of the DNS Server                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Domain name         | URL for the domain name.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| SNTP Server         | IPv6 address of the SNTP (Simple Network Time Protocol) Server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Option Code         | DHCP Option code (see RFC 2132).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Option Value        | DHCP Option value type (see RFC 2132).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

**Related commands**    [ipv6 dhcp pool](#)

# sntp-address

**Overview** Use this command in DHCPv6 Configuration mode to add an SNTP Server IPv6 address to a DHCPv6 Server pool.

Use the **no** variant of this command to remove an SNTP Server IPv6 address from a DHCPv6 Server pool.

**Syntax** `sntp-address <ipv6-address>`  
`no sntp-address <ipv6-address>`

| Parameter                         | Description                                                                          |
|-----------------------------------|--------------------------------------------------------------------------------------|
| <code>&lt;ipv6-address&gt;</code> | Specify an SNTP Server IPv6 address, in hexadecimal notation in the format X:X::X:X. |

**Mode** DHCPv6 Configuration

**Examples** The following example adds an SNTP Server IPv6 address of 2001:0db8::/32 to the DHCPv6 pool named P2:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# sntp-address 2001:0db8::/32
```

The following example removes an SNTP Server IPv6 address of 2001:0db8::/32 to the DHCPv6 pool named P2:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# no sntp-address 2001:0db8::/32
```

**Related commands**

- [dns-server \(DHCPv6\)](#)
- [domain-name \(DHCPv6\)](#)
- [option \(DHCPv6\)](#)
- [show ipv6 dhcp pool](#)

# 47

# Download Portal Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure Download Portal.

The Download Portal provides a mechanism for administrators to offer resources to network users, protected by authentication. The resources could include software installers and setup guidelines, for example a remote access client along with setup instructions.

For more information, see the [Download Portal Feature Overview and Configuration Guide](#).

- Command List**
- [“aaa authentication download-portal”](#) on page 2296
  - [“download-portal”](#) on page 2298
  - [“download-portal reload”](#) on page 2299
  - [“enable \(download-portal\)”](#) on page 2300
  - [“file \(download-portal\)”](#) on page 2301
  - [“http listen”](#) on page 2303
  - [“http secure-listen”](#) on page 2305
  - [“secure-listen \(download-portal\)”](#) on page 2307
  - [“show download-portal”](#) on page 2309
  - [“uri \(download-portal\)”](#) on page 2310

# aaa authentication download-portal

**Overview** Use this command to globally enable authentication, and set the default authentication method, for Download Portal clients. The default authentication method can be:

- all configured RADIUS servers,
- all configured LDAP servers,
- or a user-defined group of RADIUS or LDAP servers.

Use the **no** variant of this command to globally disable authentication on for Download Portal Clients.

**Syntax** `aaa authentication download-portal default group  
[<group-name>|radius|ldap]  
no aaa authentication download-portal default`

| Parameter    | Description            |
|--------------|------------------------|
| <group-name> | Server group name.     |
| radius       | Use all RADIUS servers |
| ldap         | Use all LDAP servers   |

**Default** Authentication for Download Portal clients is disabled by default.

**Mode** Global Configuration

**Usage notes** There are a number of ways to define groups of authentication servers. These are:

- **group radius:** use all RADIUS servers configured with the [radius-server host](#) command.
- **group ldap:** use all LDAP servers configured with the [ldap-server](#) command.
- **group <group-name>:** use the specified RADIUS or LDAP server group configured with the [aaa group server](#) command.

**Example** To enable LDAP authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication download-portal default
group ldap
```

To use a server group to authenticate Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication download-portal default
group my_group
```

**Note:** This could be a group of RADIUS or LDAP servers.

To disable authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication download-portal default
```

**Related  
commands**

[aaa group server](#)  
[download-portal](#)

**Command  
changes**

Version 5.5.4-0: command added

# download-portal

**Overview** Use this command to enter Download Portal configuration mode.  
Use the **no** variant of this command to remove all Download Portal configuration.

**Syntax** `download-portal`  
`no download-portal`

**Mode** Global Configuration

**Usage notes** The Download Portal enables AlliedWare Plus administrators to provide resources to authenticated network users. These resources may include software installers and setup guidelines, such as a remote access client with accompanying instructions. The resources offered are curated and configured by AlliedWare Plus administrators.

**Example** To enter Download Portal configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)#
```

To remove all Download Portal configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no download-portal
awplus(config)#
```

**Related commands** [enable \(download-portal\)](#)  
[secure-listen \(download-portal\)](#)  
[file \(download-portal\)](#)  
[uri \(download-portal\)](#)  
[show download-portal](#)

**Command changes** Version 5.5.4-0: command added

# download-portal reload

**Overview** Use this command to reload the Download Portal which will recreate the Download Portal page.

**Syntax** `download-portal reload`

**Mode** Privileged Exec

**Usage Notes** This is necessary if your device supports external media, such as a USB or SD card, and files are configured from the external media while the external media is not plugged in. When the external media is plugged in the Download Portal page is not automatically reloaded so the files will not appear. Use this command to force a reload.

**Example** To reload the Download Portal page, use the command:

```
awplus# download-portal reload
```

**Related commands** [download-portal](#)

**Command changes** Version 5.5.4-0: command added

# enable (download-portal)

**Overview** Use this command to enable the Download Portal.  
Use the **no** variant of this command to disable the Download Portal.

**Syntax** enable  
no enable

**Default** Not enabled.

**Mode** Download Portal Configuration

**Example** To enable the Download Portal, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# enable
```

To disable the Download Portal, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no enable
```

**Related commands** [download-portal](#)

**Command changes** Version 5.5.4-0: command added



# file (download-portal)

**Overview** Use this command to configure a file that will be displayed in the Download Portal page.

Use the **no** variant of this command to remove a file from the Download Portal page.

**Syntax** `file <file-path> [sha256sum <hex-string>] [description <file-description>]`  
`no file <file-path> [sha256sum <hex-string>] [description <file-description>]`

| Parameter   | Description                                                                                                                                                                         |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <file-path> | The path to the file to be made available in the Download Portal. This file must be present in Flash, USB, or SD card storage.                                                      |
| sha256sum   | Optionally, provide the sha256sum of the file. If configured, then this is checked against the file and if it does not match, then it is not displayed on the Download Portal page. |
| description | Optionally provide a description for the file to be presented to the user accessing the Download Portal page                                                                        |

**Mode** Download Portal Configuration

**Usage notes** The file path must be specific, such as starts with "flash:/"(Flash), "usb:/"(USB), or "card:/"(SDcard):

- If the file path is incorrect, the configured file does not show on the Download Portal page.
- The checksum of the file is optional, but if the configured value is not matched, the file will not be shown on the Download Portal page.
- Description is optional, it helps users understand what the file is about.

**Example** To configure files for the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# file flash:/staff.txt
sha256sum albed1569bef6b9f8958bf8993ef53bf7c2f62a1833fe41f14
description "Staff List"
awplus(config-download-portal)# file usb:/3g.bin description
"3G file for testing purpose"
awplus(config-download-portal)# file card:/default.cfg
description "Default Configuration File"
```

To remove a file from the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no file flash:/staff.txt
```

**Related  
commands**

[download-portal](#)  
[download-portal reload](#)

**Command  
changes**

Version 5.5.4-0: command added

# http listen

**Overview** Use this command to configure the HTTP service to stop listening on all addresses and, instead, listen on a specific address and port.

Use the **no** variant of this command to remove an address and port that the HTTP service was listening on.

**Syntax** `http listen {<ip-address>|<ipv6-address>} <1-65535>`  
`no http listen {<ip-address>|<ipv6-address>} <1-65535>`

| Parameter      | Description                                                                               |
|----------------|-------------------------------------------------------------------------------------------|
| <ip-address>   | Specify the IPv4 address to listen on for HTTP connections, entered in the form A.B.C.D.  |
| <ipv6-address> | Specify the IPv6 address to listen on for HTTP connections, entered in the form X:X::X:X. |
| <1-65535>      | The TCP port to listen on for HTTP connections.                                           |

**Mode** Privileged Exec

**Usage notes** AlliedWare Plus devices are configured by default to allow access to the HTTP service using the default HTTP port 80 from any configured address on the device.

However, you can configure the HTTP service to listen on a specific address and port by using the **http listen** command in combination with the **http port none** command. Note, the IP specified must already be configured on the interface that you want to listen on.

These two commands help to ensure the AlliedWare Plus HTTP service is only reachable on a particular interface. It is recommended that the AlliedWare Plus HTTP service is not accessible from the Internet and/or firewall rules are configured to only allow access from trusted IP networks.

**Example** To disable the HTTP service listening on all addresses and instead listen on a specific address and port, use the commands:

```
awplus# configure terminal
awplus(config)# http port none
awplus(config)# http listen 192.168.1.1 10080
```

To remove an address and port that the HTTP service was listening on, use the commands:

```
awplus# configure terminal
awplus(config)# no http listen 192.168.1.1 10080
```

**Related commands** [download-portal](#)

**Command changes** Version 5.5.4-0: command added

# http secure-listen

**Overview** Use this command to configure the HTTPS service to stop listening on all addresses and instead listen on a specific address and port.

Use the **no** variant of this command to remove an address and port that the HTTPS service was listening on.

**Syntax** `http secure-listen {<ip-address>|<ipv6-address>} <1-65535>`  
`no http secure-listen {<ip-address>|<ipv6-address>} <1-65535>`

| Parameter      | Description                                                                                |
|----------------|--------------------------------------------------------------------------------------------|
| <ip-address>   | Specify the IPv4 address to listen on for HTTPS connections, entered in the form A.B.C.D.  |
| <ipv6-address> | Specify the IPv6 address to listen on for HTTPS connections, entered in the form X:X::X:X. |
| <1-65535>      | The TCP port to listen on for HTTPS connections.                                           |

**Mode** Privileged Exec

**Usage notes** By default, AlliedWare Plus devices are configured to allow access to the HTTPS service on the default HTTPS port 443 from any configured address on the device.

However, you can configure the HTTPS service to listen on a specific address and port by using the **http secure-listen** command in combination with the **http secure-port none** command. Note, the IP specified must already be configured on the interface that you want to listen on.

These two 'http' commands help ensure the AlliedWare Plus HTTPS service is only reachable on a particular interface. We recommend that the AlliedWare Plus HTTPS service is not accessible from the Internet and/or firewall rules are configured to only allow access from trusted IP networks.

**Example** To stop the HTTPS service listening on all addresses and instead listen on a specific address and port, use the commands:

```
awplus# configure terminal
awplus(config)# http secure-port none
awplus(config)# http secure-listen 192.168.1.1 10443
```

To remove an address and port that the HTTPS service was listening on, use the commands:

```
awplus# configure terminal
awplus(config)# no http secure-listen 192.168.1.1 10080
```

**Related commands** [download-portal](#)

**Command changes** Version 5.5.4-0: command added

# secure-listen (download-portal)

**Overview** Use this command to add an address and port for the Download Portal to listen on for HTTPS connections.

Use the **no** variant of this command to remove a secure listen address and port.

**Syntax** `secure-listen {<ip-address>|<ipv6-address>} <1-65535>`  
`no secure-listen {<ip-address>|<ipv6-address>} <1-65535>`

| Parameter      | Description                                                                                |
|----------------|--------------------------------------------------------------------------------------------|
| <ip-address>   | Specify the IPv4 address to listen on for HTTPS connections, entered in the form A.B.C.D.  |
| <ipv6-address> | Specify the IPv6 address to listen on for HTTPS connections, entered in the form X:X::X:X. |
| <1-65535>      | TCP port to listen on for HTTPS connections.                                               |

**Mode** Download Portal Configuration

**Usage notes** By default, the Download Portal cannot be accessed because it is not listening on any port for HTTP or HTTPS client connections. The **secure-listen** command must be configured to set the addresses and ports that the Download Portal HTTP service will listen on for clients connections. The IP specified must be configured on an interface.

It is recommended that the firewall rules are configured to ensure that the Download Portal is only reachable by clients that you expect.

**Example** To add an address and port for the Download Portal to listen on for HTTPS connections, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# secure-listen 192.168.2.45
10443
```

To remove an address and port that the Download Portal was listening on for HTTPS connections, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no secure-listen 192.168.2.45
10443
```

**Related commands** [download-portal](#)

**Command changes** Version 5.5.4-0: command added



# show download-portal

**Overview** Use this command to show the current status of the Download Portal and display the total configured files and URIs (Uniform Resource Identifiers).

**Syntax** `show download-portal`

**Mode** Privileged Exec

**Example** To show the number of configured URIs and files for the Download Portal, use the command:

```
awplus# show download-portal
```

**Output** Figure 47-1: Example output from **show download-portal**

```
awplus#show download-portal
Status: Enabled
Files: 2
Secure-listen Addresses:
192.168.1.15:8443
```

**Related commands** [download-portal](#)

**Command changes** Version 5.5.4-0: command added

# uri (download-portal)

**Overview** Use this command to configure a URI (Uniform Resource Identifier) that links to an external resource to be displayed on the Download Portal page.

Use the **no** variant of this command to remove the URI link from the Download Portal page.

**Syntax** `uri <uri-link> [description <uri-description>]`  
`no uri <uri-link>`

| Parameter                            | Description                                                                                           |
|--------------------------------------|-------------------------------------------------------------------------------------------------------|
| <code>&lt;uri-link&gt;</code>        | The URI link to be displayed. It must have a protocol prefix, such as: "https://" or "mailto://"      |
| <code>&lt;uri-description&gt;</code> | Optionally provide a description for the URI to be presented to the user on the Download Portal page. |

**Mode** Download Portal Configuration

**Example** To set a URI with a description for the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# uri https://alliedtelesis.com
description Company Page
```

To remove a URI for the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no uri
https://alliedtelesis.com
```

**Related commands** [download-portal](#)

**Command changes** Version 5.5.4-0: command added

# 48

# SNMP Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure SNMP. For more information, see:

- the [Support for Allied Telesis Enterprise\\_MIBs in AlliedWare Plus](#), for information about which MIB objects are supported.
- the [SNMP Feature Overview and Configuration\\_Guide](#).

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Command List**
- [“alias \(interface\)”](#) on page 2313
  - [“debug snmp”](#) on page 2314
  - [“show counter snmp-server”](#) on page 2315
  - [“show debugging snmp”](#) on page 2319
  - [“show running-config snmp”](#) on page 2320
  - [“show snmp-server”](#) on page 2321
  - [“show snmp-server community”](#) on page 2322
  - [“show snmp-server group”](#) on page 2323
  - [“show snmp-server trap”](#) on page 2324
  - [“show snmp-server user”](#) on page 2325
  - [“show snmp-server view”](#) on page 2326
  - [“snmp trap link-status”](#) on page 2327
  - [“snmp trap link-status suppress”](#) on page 2328
  - [“snmp-server”](#) on page 2330
  - [“snmp-server community”](#) on page 2332
  - [“snmp-server contact”](#) on page 2333

- [“snmp-server enable trap”](#) on page 2334
- [“snmp-server engineID local”](#) on page 2337
- [“snmp-server engineID local reset”](#) on page 2339
- [“snmp-server group”](#) on page 2340
- [“snmp-server host”](#) on page 2342
- [“snmp-server legacy-ifadminstatus”](#) on page 2344
- [“snmp-server location”](#) on page 2345
- [“snmp-server source-interface”](#) on page 2346
- [“snmp-server startup-trap-delay”](#) on page 2347
- [“snmp-server user”](#) on page 2348
- [“snmp-server view”](#) on page 2351
- [“test snmp trap snmp”](#) on page 2352
- [“undebbug snmp”](#) on page 2353

# alias (interface)

**Overview** Use this command to set an alias name for a port, as returned by the SNMP ifMIB in OID 1.3.6.1.2.1.31.1.1.1.18.

Use the **no** variant of this command to remove an alias name from a port.

**Syntax** `alias <ifAlias>`  
`no alias`

| Parameter | Description                                                                                            |
|-----------|--------------------------------------------------------------------------------------------------------|
| <ifAlias> | 64 character name for an interface in a network management system. All printable characters are valid. |

**Default** Not set.

**Mode** Interface Configuration

**Usage notes** The interface alias can also be set via SNMP.  
Third-party management systems often use standard MIBs to access device information. Network managers can specify an alias interface name to provide a non-volatile way to access the interface.

**Example** To configure the alias interface name 'uplink\_a' for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# alias uplink_a
```

To remove an alias interface name from eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no alias
```

**Command changes** Version 5.4.8-2.1: command added

# debug snmp

**Overview** This command enables SNMP debugging.  
The **no** variant of this command disables SNMP debugging.

**Syntax** debug snmp  
[all|detail|error-string|process|receive|send|xdump]  
no debug snmp  
[all|detail|error-string|process|receive|send|xdump]

| Parameter    | Description                                                                               |
|--------------|-------------------------------------------------------------------------------------------|
| all          | Enable or disable the display of all SNMP debugging information.                          |
| detail       | Enable or disable the display of detailed SNMP debugging information.                     |
| error-string | Enable or disable the display of debugging information for SNMP error strings.            |
| process      | Enable or disable the display of debugging information for processed SNMP packets.        |
| receive      | Enable or disable the display of debugging information for received SNMP packets.         |
| send         | Enable or disable the display of debugging information for sent SNMP packets.             |
| xdump        | Enable or disable the display of hexadecimal dump debugging information for SNMP packets. |

**Mode** Privileged Exec and Global Configuration

**Example** To start SNMP debugging, use the command:

```
awplus# debug snmp
```

To start SNMP debugging, showing detailed SNMP debugging information, use the command:

```
awplus# debug snmp detail
```

To start SNMP debugging, showing all SNMP debugging information, use the command:

```
awplus# debug snmp all
```

**Related commands** [show debugging snmp](#)  
[terminal monitor](#)  
[undebug snmp](#)

# show counter snmp-server

**Overview** This command displays counters for SNMP messages received by the SNMP agent.

**Syntax** `show counter snmp-server`

**Mode** User Exec and Privileged Exec

**Example** To display the counters for the SNMP agent, use the command:

```
awplus# show counter snmp-server
```

**Output** Figure 48-1: Example output from the **show counter snmp-server** command

```
SNMP-SERVER counters
inPkts 11
inBadVersions 0
inBadCommunityNames 0
inBadCommunityUses 0
inASNParseErrs 0
inTooBigs 0
inNoSuchNames 0
inBadValues 0
inReadOnlys 0
inGenErrs 0
inTotalReqVars 9
inTotalSetVars 0
inGetRequests 2
inGetNexts 9
inSetRequests 0
inGetResponses 0
inTraps 0
outPkts 11
outTooBigs 0
outNoSuchNames 2
outBadValues 0
outGenErrs 0
outGetRequests 0
outGetNexts 0
outSetRequests 0
outGetResponses 11
outTraps 0
UnsupportedSecLevels 0
NotInTimeWindows 0
UnknownUserNames 0
UnknownEngineIDs 0
WrongDigest 0
DecryptionErrors 0
UnknownSecModels 0
InvalidMsgs 0
UnknownPDUHandlers 0
```

**Table 1:** Parameters in the output of the **show counter snmp-server** command

| Parameter           | Meaning                                                                                                                                                                                                                                                                                            |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| inPkts              | The total number of SNMP messages received by the SNMP agent.                                                                                                                                                                                                                                      |
| inBadVersions       | The number of messages received by the SNMP agent for an unsupported SNMP version. It drops these messages. The SNMP agent on your device supports versions 1, 2C, and 3.                                                                                                                          |
| inBadCommunityNames | The number of messages received by the SNMP agent with an unrecognized SNMP community name. It drops these messages.                                                                                                                                                                               |
| inBadCommunityUses  | The number of messages received by the SNMP agent where the requested SNMP operation is not permitted from SNMP managers using the SNMP community named in the message.                                                                                                                            |
| inASNParseErrs      | The number of ASN.1 or BER errors that the SNMP agent has encountered when decoding received SNMP Messages.                                                                                                                                                                                        |
| inTooBigs           | The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'tooBig'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.                                                                         |
| inNoSuchNames       | The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'noSuchName'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.                                                                     |
| inBadValues         | The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'badValue'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.                                                                       |
| inReadOnlys         | The number of valid SNMP PDUs received by the SNMP agent where the value of the error-status field is 'readOnly'. The SNMP manager should not generate a PDU which contains the value 'readOnly' in the error-status field. This indicates that there is an incorrect implementations of the SNMP. |
| inGenErrs           | The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'genErr'.                                                                                                                                                                                          |



**Table 1:** Parameters in the output of the **show counter snmp-server** command

| Parameter      | Meaning                                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| inTotalReqVars | The number of MIB objects that the SNMP agent has successfully retrieved after receiving valid SNMP Get-Request and Get-Next PDUs.                                                                                                   |
| inTotalSetVars | The number of MIB objects that the SNMP agent has successfully altered after receiving valid SNMP Set-Request PDUs.                                                                                                                  |
| inGetRequests  | The number of SNMP Get-Request PDUs that the SNMP agent has accepted and processed.                                                                                                                                                  |
| inGetNexts     | The number of SNMP Get-Next PDUs that the SNMP agent has accepted and processed.                                                                                                                                                     |
| inSetRequests  | The number of SNMP Set-Request PDUs that the SNMP agent has accepted and processed.                                                                                                                                                  |
| inGetResponses | The number of SNMP Get-Response PDUs that the SNMP agent has accepted and processed.                                                                                                                                                 |
| inTraps        | The number of SNMP Trap PDUs that the SNMP agent has accepted and processed.                                                                                                                                                         |
| outPkts        | The number of SNMP Messages that the SNMP agent has sent.                                                                                                                                                                            |
| outTooBigs     | The number of SNMP PDUs that the SNMP agent has generated with the value 'tooBig' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.     |
| outNoSuchNames | The number of SNMP PDUs that the SNMP agent has generated with the value 'noSuchName' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager. |
| outBadValues   | The number of SNMP PDUs that the SNMP agent has generated with the value 'badValue' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.   |
| outGenErrs     | The number of SNMP PDUs that the SNMP agent has generated with the value 'genErr' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.     |
| outGetRequests | The number of SNMP Get-Request PDUs that the SNMP agent has generated.                                                                                                                                                               |

**Table 1:** Parameters in the output of the **show counter snmp-server** command

| Parameter            | Meaning                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| outGetNexts          | The number of SNMP Get-Next PDUs that the SNMP agent has generated.                                                                               |
| outSetRequests       | The number of SNMP Set-Request PDUs that the SNMP agent has generated.                                                                            |
| outGetResponses      | The number of SNMP Get-Response PDUs that the SNMP agent has generated.                                                                           |
| outTraps             | The number of SNMP Trap PDUs that the SNMP agent has generated.                                                                                   |
| UnsupportedSecLevels | The number of received packets that the SNMP agent has dropped because they requested a securityLevel unknown or not available to the SNMP agent. |
| NotInTimeWindows     | The number of received packets that the SNMP agent has dropped because they appeared outside of the authoritative SNMP agent's window.            |
| UnknownUserNames     | The number of received packets that the SNMP agent has dropped because they referenced an unknown user.                                           |
| UnknownEngineIDs     | The number of received packets that the SNMP agent has dropped because they referenced an unknown snmpEngineID.                                   |
| WrongDigest          | The number of received packets that the SNMP agent has dropped because they didn't contain the expected digest value.                             |
| DecryptionErrors     | The number of received packets that the SNMP agent has dropped because they could not be decrypted.                                               |
| UnknownSecModels     | The number of messages received that contain a security model that is not supported by the server. Valid for SNMPv3 messages only.                |
| InvalidMsgs          | The number of messages received where the security model is supported but the authentication fails. Valid for SNMPv3 messages only.               |
| UnknownPDUHandlers   | The number of times the SNMP handler has failed to process a PDU. This is a system debugging counter.                                             |

**Related commands** [show snmp-server](#)

# show debugging snmp

**Overview** This command displays whether SNMP debugging is enabled or disabled.

**Syntax** `show debugging snmp`

**Mode** User Exec and Privileged Exec

**Example** To display the status of SNMP debugging, use the command:

```
awplus# show debugging snmp
```

**Output** Figure 48-2: Example output from the **show debugging snmp** command

```
Sntp (SMUX) debugging status:
Sntp debugging is on
```

**Related commands** [debug snmp](#)

# show running-config snmp

**Overview** This command displays the current configuration of SNMP on your device.

**Syntax** `show running-config snmp`

**Mode** Privileged Exec

**Example** To display the current configuration of SNMP on your device, use the command:

```
awplus# show running-config snmp
```

**Output** Figure 48-3: Example output from the **show running-config snmp** command

```
snmp-server contact AlliedTelesis
snmp-server location Philippines
snmp-server group grou1 auth read view1 write view1 notify view1
snmp-server view view1 1 included
snmp-server community public
snmp-server user user1 group1 auth md5 password priv des
password
```

**Related commands** [show snmp-server](#)

# show snmp-server

**Overview** This command displays the status and current configuration of the SNMP server.

**Syntax** `show snmp-server`

**Mode** Privileged Exec

**Example** To display the status of the SNMP server, use the command:

```
awplus# show snmp-server
```

**Output** Figure 48-4: Example output from the **show snmp-server** command

```
SNMP Server Enabled
IP Protocol IPv4
SNMPv3 Engine ID (configured name) ... Not set
SNMPv3 Engine ID (actual) 0x80001f888021338e4747b8e607
```

**Related commands**

- [debug snmp](#)
- [show counter snmp-server](#)
- [snmp-server](#)
- [snmp-server engineID local](#)
- [snmp-server engineID local reset](#)

# show snmp-server community

**Overview** This command displays the SNMP server communities configured on the device. SNMP communities are specific to v1 and v2c.

**Syntax** `show snmp-server community`

**Mode** Privileged Exec

**Example** To display the SNMP server communities, use the command:

```
awplus# show snmp-server community
```

**Output** Figure 48-5: Example output from the **show snmp-server community** command

```
SNMP community information:
Community Name public
Access Read-only
View none
```

**Related commands** [show snmp-server](#)  
[snmp-server community](#)

# show snmp-server group

**Overview** This command displays information about SNMP server groups. This command is used with SNMP version 3 only.

**Syntax** `show snmp-server group`

**Mode** Privileged Exec

**Example** To display the SNMP groups configured on the device, use the command:

```
awplus# show snmp-server group
```

**Output** Figure 48-6: Example output from the **show snmp-server group** command

```
SNMP group information:
 Group name guireadgroup
 Security Level priv
 Read View guiview
 Write View none
 Notify View none

 Group name guiwritegroup
 Security Level priv
 Read View none
 Write View guiview
 Notify View none
```

**Related commands** [show snmp-server](#)  
[snmp-server group](#)

# show snmp-server trap

**Overview** Use this command to display the status of the SNMP traps.

**Syntax** show snmp-server trap

**Mode** Privileged Exec

**Example** To display the SNMP traps status, use the commands:

```
awplus# show snmp-server trap
```

**Output** Figure 48-7: Example output from **show snmp-server trap**

```
awplus#show snmp-server trap
ATMF traps Disabled
ATMF Link traps Disabled
ATMF Node traps Disabled
ATMF Guest Node traps Enabled
ATMF Reboot Rolling traps Disabled
Authentication failure Disabled
BGP traps Disabled
CWM Access Point traps Enabled
DHCP Snooping traps Disabled
EPSR traps Disabled
LLDP traps Disabled
Loop Protection traps Disabled
MSTP traps Disabled
NSM traps Disabled
OSPF traps Disabled
PIM traps Disabled
Power-inline traps Disabled
QoS Storm Protection traps Enabled
RMON traps Disabled
MAC address Thrash Limiting traps Disabled
UDLD traps Disabled
VCS traps Disabled
VRRP traps Disabled
Wireless traps Disabled
```

**Related commands** [show snmp-server](#)  
[snmp-server enable trap](#)



# show snmp-server user

**Overview** This command displays the SNMP server users and is used with SNMP version 3 only.

**Syntax** `show snmp-server user`

**Mode** Privileged Exec

**Example** To display the SNMP server users configured on the device, use the command:

```
awplus# show snmp-server user
```

**Output** Figure 48-8: Example output from the **show snmp-server user** command

| Name   | Group name   | Auth  | Privacy |
|--------|--------------|-------|---------|
| -----  | -----        | ----- | -----   |
| freddy | guireadgroup | none  | none    |

**Related commands** [show snmp-server](#)  
[snmp-server user](#)

# show snmp-server view

**Overview** This command displays the SNMP server views and is used with SNMP version 3 only.

**Syntax** `show snmp-server view`

**Mode** Privileged Exec

**Example** To display the SNMP server views configured on the device, use the command:

```
awplus# show snmp-server view
```

**Output** Figure 48-9: Example output from the **show snmp-server view** command

```
SNMP view information:
View Name view1
OID 1
Type included
```

**Related commands** [show snmp-server](#)  
[snmp-server view](#)

# snmp trap link-status

**Overview** Use this command to enable SNMP to send link status notifications (traps) for the interfaces when an interface goes up (linkUp) or down (linkDown).

Use the **no** variant of this command to disable the sending of link status notifications.

**Syntax** `snmp trap link-status [enterprise]`  
`no snmp trap link-status`

| Parameter  | Description                                          |
|------------|------------------------------------------------------|
| enterprise | Send an Allied Telesis enterprise type of link trap. |

**Default** Disabled

**Mode** Interface Configuration

**Usage notes** The link status notifications can be enabled for the following interface types:

- Ethernet (e.g. eth0)

To specify where notifications are sent, use the [snmp-server host](#) command. To configure the device globally to send other notifications, use the [snmp-server enable trap](#) command.

**Examples** To enable SNMP to send link status notifications for eth0 use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# snmp trap link-status
```

To disable the sending of link status notifications for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no snmp trap link-status
```

**Related commands** [show interface](#)  
[snmp trap link-status suppress](#)  
[snmp-server enable trap](#)  
[snmp-server host](#)

# snmp trap link-status suppress

**Overview** Use this command to enable the suppression of link status notifications (traps) for the interfaces beyond the specified threshold, in the specified interval.

Use the **no** variant of this command to disable the suppression of link status notifications for the ports.

**Syntax** `snmp trap link-status suppress {time {<1-60>|default}|threshold {<1-20>|default}}`  
`no snmp trap link-status suppress`

| Parameter | Description                                                                                                                                                                                       |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| time      | Set the suppression timer for link status notifications.                                                                                                                                          |
| <1-60>    | The suppress time in seconds.                                                                                                                                                                     |
| default   | The default suppress time in seconds (60).                                                                                                                                                        |
| threshold | Set the suppression threshold for link status notifications. This is the number of link status notifications after which to suppress further notifications within the suppression timer interval. |
| <1-20>    | The number of link status notifications.                                                                                                                                                          |
| default   | The default number of link status notifications (20).                                                                                                                                             |

**Default** By default, if link status notifications are enabled (they are enabled by default), the suppression of link status notifications is enabled: notifications that exceed the notification threshold (default 20) within the notification timer interval (default 60 seconds) are not sent.

**Mode** Interface Configuration

**Usage notes** An unstable network can generate many link status notifications. When notification suppression is enabled, a suppression timer is started when the first link status notification of a particular type (linkUp or linkDown) is sent for an interface.

If the threshold number of notifications of this type is sent before the timer reaches the suppress time, any further notifications of this type generated for the interface during the interval are not sent. At the end of the interval, the sending of link status notifications resumes, until the threshold is reached in the next interval.

**Examples** To suppress link- status notifications for eth0 after 10 notifications in 40 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# snmp trap link-status suppress time 40
threshold 10
```

To stop suppressing link status notifications for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no snmp trap link-status suppress
```

**Related  
commands**

[show interface](#)  
[snmp trap link-status](#)

# snmp-server

**Overview** Use this command to enable the SNMP agent (server) on the device. The SNMP agent receives and processes SNMP packets sent to the device, and generates notifications (traps) that have been enabled by the [snmp-server enable trap](#) command.

Use the **no** variant of this command to disable the SNMP agent on the device. When SNMP is disabled, SNMP packets received by the device are discarded, and no notifications are generated. This does not remove any existing SNMP configuration.

**Syntax** `snmp-server [ip|ipv6]`  
`no snmp-server [ip|ipv6]`

| Parameter | Description                                |
|-----------|--------------------------------------------|
| ip        | Enable or disable the SNMP agent for IPv4. |
| ipv6      | Enable or disable the SNMP agent for IPv6. |

**Default** By default, the SNMP agent is enabled for both IPv4 and IPv6. If neither the **ip** parameter nor the **ipv6** parameter is specified for this command, then SNMP is enabled or disabled for both IPv4 and IPv6.

**Mode** Global Configuration

**Examples** To enable SNMP on the device for both IPv4 and IPv6, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server
```

To enable the SNMP agent for IPv4 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server ip
```

To disable the SNMP agent for both IPv4 and IPv6 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-server
```

To disable the SNMP agent for IPv4, use the commands:

```
awplus(config)# no snmp-server ipv4
```

**Related commands**

- [show snmp-server](#)
- [show snmp-server community](#)
- [show snmp-server user](#)
- [snmp-server community](#)
- [snmp-server contact](#)
- [snmp-server enable trap](#)
- [snmp-server engineID local](#)
- [snmp-server group](#)
- [snmp-server host](#)
- [snmp-server location](#)
- [snmp-server view](#)

# snmp-server community

**Overview** This command creates an SNMP community, optionally setting the access mode for the community. The default access mode is read-only. If the view parameter is not specified, the community allows access to all the MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used when operating SNMPv3.

The **no** variant of this command removes an SNMP community. The specified community must already exist on the device.

**Syntax** `snmp-server community <community-name> [view <view-name>|ro|rw]`  
`no snmp-server community <community-name>`

| Parameter        | Description                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------|
| <community-name> | Community name. The community name is a case sensitive string of up to 20 characters.              |
| view             | Configure SNMP view. If view is not specified, the community allows access to all the MIB objects. |
| <view-name>      | View name. The view name is a string up to 20 characters long and is case sensitive.               |
| ro               | Read-only community.                                                                               |
| rw               | Read-write community.                                                                              |

**Default** The default access mode is Read-only.

**Mode** Global Configuration

**Example** Use the following commands to create an SNMP community called 'public' with read-only access to all MIB variables from any management station:

```
awplus# configure terminal
awplus(config)# snmp-server community public ro
```

Use the following commands to remove an SNMP community called 'public'

```
awplus# configure terminal
awplus(config)# no snmp-server community public
```

**Related commands** [show snmp-server](#)  
[show snmp-server community](#)  
[snmp-server view](#)



# snmp-server contact

**Overview** This command sets the contact information for the system. The contact name is:

- displayed in the output of the [show system](#) command
- stored in the MIB object sysContact

The **no** variant of this command removes the contact information from the system.

**Syntax** `snmp-server contact <contact-info>`  
`no snmp-server contact`

| Parameter                         | Description                                                                                                                     |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;contact-info&gt;</code> | The contact information for the system, from 0 to 255 characters long. Valid characters are any printable character and spaces. |

**Mode** Global Configuration

**Example** To set the system contact information to “support@alliedtelesis.co.nz”, use the command:

```
awplus# configure terminal
awplus(config)# snmp-server contact
support@alliedtelesis.co.nz
```

**Related commands** [show system](#)  
[snmp-server location](#)  
[snmp-server group](#)

# snmp-server enable trap

**Overview** Use this command to enable the transmission of the specified notifications (traps) on your device.

Note that the Environmental Monitoring traps defined in the AT-ENVMONv2-MIB are enabled by default.

Use the **no** variant of this command to disable the transmission of the specified notifications.

**Syntax** `snmp-server enable trap <trap-list>`  
`no snmp-server enable trap <trap-list>`

Depending on your device model, you can enable some or all of the traps in the following table:

| Parameter     | Description                                                                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| atmf          | AMF traps.                                                                                                                                                                          |
| atmfguestnode | AMF guest node traps.                                                                                                                                                               |
| atmflink      | AMF link traps.                                                                                                                                                                     |
| atmfnode      | AMF node traps.                                                                                                                                                                     |
| atmfrr        | AMF reboot-rolling traps.                                                                                                                                                           |
| auth          | Authentication failure.                                                                                                                                                             |
| bgp           | BGP traps.                                                                                                                                                                          |
| chassis       | Chassis traps.                                                                                                                                                                      |
| cwmap         | Access Point traps with the AWC wireless manager.                                                                                                                                   |
| dhcpsnooping  | DHCP snooping and ARP security traps. These notifications must also be set using the <b>ip dhcp snooping violation</b> command, and/or the <b>arp security violation</b> command.   |
| epsr          | EPSR traps.                                                                                                                                                                         |
| g8032         | G.8032 ERP traps.                                                                                                                                                                   |
| lldp          | Link Layer Discovery Protocol (LLDP) traps. These notifications must also be enabled using the <b>lldp notifications</b> command, and/or the <b>lldp med-notifications</b> command. |
| loopprot      | Loop Protection traps.                                                                                                                                                              |

| Parameter     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| low-memory    | Traps that are generated when available memory drops beneath low, very low, and critical thresholds, and when it returns to normal. The traps are: <ul style="list-style-type: none"> <li>1.3.6.1.4.1.207.8.4.4.3.7.0 memoryTraps</li> <li>1.3.6.1.4.1.207.8.4.4.3.7.0.1 memoryLowTrap</li> <li>1.3.6.1.4.1.207.8.4.4.3.7.0.2 memoryVeryLowTrap</li> <li>1.3.6.1.4.1.207.8.4.4.3.7.0.3 memoryCriticalTrap (However, note that when the system reaches the critical memory threshold, it reboots before a trap can be sent.)</li> <li>1.3.6.1.4.1.207.8.4.4.3.7.0.4 memoryReturnToNormalTrap</li> <li>1.3.6.1.4.1.207.8.4.4.3.7.0.5 vcstackId</li> </ul> |
| mac-change    | MAC address changed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| mac-move      | MAC address moved between interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| mac-threshold | MAC address table reaches a threshold limit.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| mstp          | MSTP traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| nsm           | NSM traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ospf          | OSPF traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| pim           | PIM traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| power-inline  | Power-inline traps (Power Ethernet MIB RFC 3621).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| qsp           | QoS Storm Protection.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| rmon          | RMON traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| thrash-limit  | MAC address Thrash Limiting traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| vcs           | VCS traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| vrrp          | Virtual Router Redundancy (VRRP) traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| ufo           | Upstream Forwarding Only (UFO) traps.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

**Default** Disabled

**Mode** Global Configuration

**Usage notes** This command cannot be used to enable link status notifications globally. To enable link status notifications for particular interfaces, use the [snmp trap link-status](#) command.

To specify where notifications are sent, use the [snmp-server host](#) command.

Note that you can enable (or disable) multiple traps with a single command, by specifying a space-separated list of traps.

**Examples** To enable the device to send a notification if an AMF node changes its status, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap atmfnode
```

To enable the device to send MAC address Thrash Limiting traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap thrash-limit
```

To disable the device from sending MAC address Thrash Limiting traps, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable trap thrash-limit
```

To enable the device to send OSPF and VRRP-related traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap ospf vrrp
```

To disable OSPF traps being sent out by the device, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable trap ospf
```

**Related commands** [show snmp-server](#)  
[snmp trap link-status](#)  
[snmp-server host](#)

**Command changes** Version 5.5.4-2.3: **low-memory** parameter added  
Version 5.5.1-2.1: **mac-change**, **mac-move**, and **mac-threshold** parameters added  
Version 5.5.1-1.1: **atmfguestnode** and **cwmap** parameters added  
Version 5.4.7-2.1: **ufo** parameter added

# snmp-server engineID local

**Overview** Use this command to configure the SNMPv3 engine ID. The SNMPv3 engine ID is used to uniquely identify the SNMPv3 agent on a device when communicating with SNMP management clients. Once an SNMPv3 engine ID is assigned, this engine ID is permanently associated with the device until you change it.

Use the **no** variant of this command to set the user defined SNMPv3 engine ID to a system generated pseudo-random value by resetting the SNMPv3 engine. The **no snmp-server engineID local** command has the same effect as the **snmp-server engineID local default** command.

Note that the [snmp-server engineID local reset](#) command is used to force the system to generate a new engine ID when the current engine ID is also system generated.

**Syntax** `snmp-server engineID local {<engine-id>|default}`  
`no snmp-server engineID local`

| Parameter                      | Description                                                                                                                                                                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;engine-id&gt;</code> | Specify SNMPv3 Engine ID value, a string of up to 27 characters.                                                                                                                                                                                                                                 |
| <code>default</code>           | Set SNMPv3 engine ID to a system generated value by resetting the SNMPv3 engine, provided the current engine ID is user defined. If the current engine ID is system generated, use the <a href="#">snmp-server engineID local reset</a> command to force the system to generate a new engine ID. |

**Mode** Global Configuration

**Usage notes** All devices must have a unique engine ID which is permanently set unless it is configured by the user.

**Example** To set the SNMPv3 engine ID to 800000cf030000cd123456, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local
800000cf030000cd123456
```

To set a user defined SNMPv3 engine ID back to a system generated value, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server engineID local
```

**Output** The following example shows the engine ID values after configuration:

```
awplus(config)#snmp-server engineid local asdgdfh231234d
awplus(config)#exit
awplus#show snmp-server

SNMP Server Enabled
IP Protocol IPv4
SNMPv3 Engine ID (configured name) ... asdgdfh231234d
SNMPv3 Engine ID (actual) 0x80001f888029af52e149198483

awplus(config)#no snmp-server engineid local
awplus(config)#exit
awplus#show snmp-server

SNMP Server Enabled
IP Protocol IPv4
SNMPv3 Engine ID (configured name) ... Not set
SNMPv3 Engine ID (actual) 0x80001f888029af52e149198483
```

**Related commands**

- [show snmp-server](#)
- [snmp-server engineID local reset](#)
- [snmp-server group](#)

# snmp-server engineID local reset

**Overview** Use this command to force the device to generate a new pseudo-random SNMPv3 engine ID by resetting the SNMPv3 engine. If the current engine ID is user defined, use the [snmp-server engineID local](#) command to set SNMPv3 engine ID to a system generated value.

**Syntax** `snmp-server engineID local reset`

**Mode** Global Configuration

**Example** To force the SNMPv3 engine ID to be reset to a system generated value, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local reset
```

**Related commands** [snmp-server engineID local](#)  
[show snmp-server](#)

# snmp-server group

**Overview** This command is used with SNMP version 3 only, and adds an SNMP group, optionally setting the security level and view access modes for the group. The security and access views defined for the group represent the minimum required of its users in order to gain access.

The **no** variant of this command deletes an SNMP group, and is used with SNMPv3 only. The group with the specified authentication/encryption parameters must already exist.

**Syntax** `snmp-server group <groupname> {auth|noauth|priv} [read <readname>|write <writename>|notify <notifysname>]`  
`no snmp-server group <groupname>`

| Parameter     | Description                                                                                 |
|---------------|---------------------------------------------------------------------------------------------|
| <groupname>   | Group name. The group name is a string up to 20 characters long and is case sensitive.      |
| auth          | Authentication.                                                                             |
| noauth        | No authentication and no encryption.                                                        |
| priv          | Authentication and encryption.                                                              |
| read          | Configure read view.                                                                        |
| <readname>    | Read view name.                                                                             |
| write         | Configure write view.                                                                       |
| <writename>   | Write view name. The view name is a string up to 20 characters long and is case sensitive.  |
| notify        | Configure notify view.                                                                      |
| <notifysname> | Notify view name. The view name is a string up to 20 characters long and is case sensitive. |

**Mode** Global Configuration

**Examples** To add SNMP group, for ordinary users, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server group usergroup noauth read
useraccess write useraccess
```

To delete the SNMP group called 'usergroup', use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server group usergroup
```



**Related  
commands**

snmp-server  
show snmp-server  
show snmp-server group  
show snmp-server user

# snmp-server host

**Overview** This command specifies an SNMP trap host destination to which Trap or Inform messages generated by the device are sent.

For SNMP version 1 and 2c you must specify the community name parameter. For SNMP version 3, specify the authentication/encryption parameters and the user name. If the version is not specified, the default is SNMP version 1. Inform messages can be sent instead of traps for SNMP version 2c and 3.

Use the **no** variant of this command to remove an SNMP trap host. The trap host must already exist.

The trap host is uniquely identified by:

- host IP address (IPv4 or IPv6)
- inform or trap messages
- community name (SNMPv1 or SNMP v2c) or the authentication/encryption parameters and user name (SNMP v3).

**Syntax**

```
snmp-server host {<ipv4-address>|<ipv6-address>} [traps]
[version 1] <community-name>

snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 2c <community-name>

snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 3 {auth|noauth|priv} <user-name>

no snmp-server host {<ipv4-address>|<ipv6-address>} [traps]
[version 1] <community-name>

no snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 2c <community-name>

no snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 3 {auth|noauth|priv} <user-name>
```

| Parameter      | Description                                                                    |
|----------------|--------------------------------------------------------------------------------|
| <ipv4-address> | IPv4 trap host address in the format A.B.C.D, for example, 192.0.2.2.          |
| <ipv6-address> | IPv6 trap host address in the format x::x::x for example, 2001:db8::8a2e:7334. |
| informs        | Send Inform messages to this host.                                             |
| traps          | Send Trap messages to this host (default).                                     |
| version        | SNMP version to use for notification messages. Default: version 1.             |
| 1              | Use SNMPv1 (default).                                                          |
| 2c             | Use SNMPv2c.                                                                   |
| 3              | Use SNMPv3.                                                                    |

| Parameter        | Description                           |
|------------------|---------------------------------------|
| auth             | Authentication.                       |
| noauth           | No authentication.                    |
| priv             | Encryption.                           |
| <community-name> | The SNMPv1 or SNMPv2c community name. |
| <user-name>      | SNMPv3 user name.                     |

**Default** No host is defined.

**Mode** Global Configuration

**Usage notes** You can test connectivity to the host by using the command [test snmp trap snmp](#).

**Examples** To configure the device to send generated traps to the IPv4 host destination 192.0.2.5 with the SNMPv2c community name 'public', use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server host 192.0.2.5 version 2c public
```

To configure the device to send generated traps to the IPv6 host destination 2001:db8::8a2e:7334 with the SNMPv2c community name 'private', use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server host 2001:db8::8a2e:7334 version 2c
private
```

To remove a configured trap host of 192.0.2.5 with the SNMPv2c community name 'public', use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server host 192.0.2.5 version 2c public
```

**Related commands**

- [snmp trap link-status](#)
- [snmp-server enable trap](#)
- [snmp-server view](#)
- [test snmp trap snmp](#)

**Command changes** Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

# snmp-server legacy-ifadminstatus

**Overview** Use this command to set the ifAdminStatus to reflect the operational state of the interface, rather than the administrative state.

The **no** variant of this command sets the ifAdminStatus to reflect the administrative state of the interface.

**Syntax** `snmp-server legacy-ifadminstatus`  
`no snmp-server legacy-ifadminstatus`

**Default** Legacy ifAdminStatus is turned off by default, so by default the SNMP ifAdminStatus reflects the administrative state of the interface.

**Mode** Global Configuration

**Usage notes** Note that if you enable Legacy ifAdminStatus, the ifAdminStatus will report a link's status as Down when the link has been blocked by a process such as loop protection.

**Example** To turn on Legacy ifAdminStatus, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server legacy-ifadminstatus
```

**Related commands** [show interface](#)

# snmp-server location

**Overview** This command sets the location of the system. The location is:

- displayed in the output of the [show system](#) command
- stored in the MIB object sysLocation

The **no** variant of this command removes the configured location from the system.

**Syntax** `snmp-server location <location-name>`  
`no snmp-server location`

| Parameter                          | Description                                                                                                         |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <code>&lt;location-name&gt;</code> | The location of the system, from 0 to 255 characters long. Valid characters are any printable character and spaces. |

**Mode** Global Configuration

**Example** To set the location to “server room 523”, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server location server room 523
```

**Related commands** [show snmp-server](#)  
[show system](#)  
[snmp-server contact](#)

# snmp-server source-interface

**Overview** Use this command to specify the originating interface for SNMP traps or informs. An interface specified by this command must already have an IP address assigned to it.

Use the **no** variant of this command to reset the interface to its default value (the originating egress interface).

**Syntax** `snmp-server source-interface {traps|informs} <interface-name>`  
`no snmp-server source-interface {traps|informs}`

| Parameter        | Description                                                |
|------------------|------------------------------------------------------------|
| traps            | SNMP traps.                                                |
| informs          | SNMP informs.                                              |
| <interface-name> | Interface name (must already have an IP address assigned). |

**Default** The originating egress interface of the traps and informs messages

**Mode** Global Configuration

**Usage notes** When an SNMP server sends an SNMP trap or inform message, the message carries the notification IP address of its originating interface. Use this command to assign this interface.

**Example** The following commands set vlan2 to be the interface whose IP address is used as the originating address in SNMP informs packets.

```
awplus# configure terminal
awplus(config)# snmp-server source-interface informs vlan2
```

The following commands reset the originating source interface for SNMP trap messages to be the default interface (the originating egress interface):

```
awplus# configure terminal
awplus(config)# no snmp-server source-interface traps
```

**Validation Commands** [show running-config](#)

# snmp-server startup-trap-delay

**Overview** Use this command to set the time in seconds after following completion of the device startup sequence before the device sends any SNMP traps (or SNMP notifications).

Use the no variant of this command to restore the default startup delay of 30 seconds.

**Syntax** `snmp-server startup-trap-delay <delay-time>`  
`no snmp-server startup-trap-delay`

| Parameter                       | Description                                                                   |
|---------------------------------|-------------------------------------------------------------------------------|
| <code>&lt;delay-time&gt;</code> | Specify an SNMP trap delay time in seconds in the range of 30 to 600 seconds. |

**Default** The SNMP server trap delay time is 30 seconds. The no variant restores the default.

**Mode** Global Configuration

**Example** To delay the device sending SNMP traps until 60 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server startup-trap-delay 60
```

To restore the sending of SNMP traps to the default of 30 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server startup-trap-delay
```

**Validation  
Commands** `show snmp-server`

## snmp-server user

**Overview** Use this command to create or move users as members of specified groups. This command is used with SNMPv3 only.

The **no** variant of this command removes an SNMPv3 user. The specified user must already exist.

**Syntax** `snmp-server user <username> <groupname> [encrypted] [auth {md5|sha} <auth-password>] [priv {des|aes} <privacy-password>]`  
`no snmp-server user <username>`

| Parameter          | Description                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------|
| <username>         | User name. The user name is a string up to 20 characters long and is case sensitive.                |
| <groupname>        | Group name. The group name is a string up to 20 characters long and is case sensitive.              |
| encrypted          | Use the encrypted parameter when you want to enter encrypted passwords.                             |
| auth               | Authentication protocol.                                                                            |
| md5                | MD5 Message Digest Algorithms.                                                                      |
| sha                | SHA Secure Hash Algorithm.                                                                          |
| <auth-password>    | Authentication password. The password is a string of 8 to 20 characters long and is case sensitive. |
| priv               | Privacy protocol.                                                                                   |
| des                | DES: Data Encryption Standard.                                                                      |
| aes                | AES: Advanced Encryption Standards.                                                                 |
| <privacy-password> | Privacy password. The password is a string of 8 to 20 characters long and is case sensitive.        |

**Mode** Global Configuration

**Usage notes** Additionally this command provides the option of selecting an authentication protocol and (where appropriate) an associated password. Similarly, options are offered for selecting a privacy protocol and password.

- Note that each SNMP user must be configured on both the manager and agent entities. Where passwords are used, these passwords must be the same for both entities.
- Use the **encrypted** parameter when you want to enter already encrypted passwords in encrypted form as displayed in the running and startup configs stored on the device. For example, you may need to move a user from one group to another group and keep the same passwords for the user instead of removing the user to apply new passwords.



- User passwords are entered using plaintext without the **encrypted** parameter and are encrypted according to the authentication and privacy protocols selected.
- User passwords are viewed as encrypted passwords in running and startup configs shown from **show running-config** and **show startup-config** commands respectively. Copy and paste encrypted passwords from running-configs or startup-configs to avoid entry errors.

**Examples** To add SNMP user authuser as a member of group 'usergroup', with authentication protocol MD5, authentication password 'Authpass', privacy protocol AES and privacy password 'Privpass' use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# snmp-server user authuser usergroup auth md5
Authpass priv aes Privpass
```

Validate the user is assigned to the group using the **show snmp-server user** command:

| awplus#show snmp-server user |            |       |         |
|------------------------------|------------|-------|---------|
| Name                         | Group name | Auth  | Privacy |
| -----                        | -----      | ----- | -----   |
| authuser                     | usergroup  | md5   | aes     |

To enter existing SNMP user 'authuser' with existing passwords as a member of group 'newusergroup' with authentication protocol MD5 with the encrypted authentication password 0x1c74b9c22118291b0ce0cd883f8dab6b74, and privacy protocol AES with the encrypted privacy password 0x0e0133db5453ebd03822b004eeacb6608f, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# snmp-server user authuser newusergroup
encrypted auth md5 0x1c74b9c22118291b0ce0cd883f8dab6b74 priv
aes 0x0e0133db5453ebd03822b004eeacb6608f
```

**NOTE:** Copy and paste the encrypted passwords from the **running-config** or the **startup-config** displayed, using the **show running-config** and **show startup-config** commands respectively, into the command line to avoid key stroke errors issuing this command.

Validate the user has been moved from the first group using the **show snmp-server user** command:

| awplus#show snmp-server user |              |       |         |
|------------------------------|--------------|-------|---------|
| Name                         | Group name   | Auth  | Privacy |
| -----                        | -----        | ----- | -----   |
| authuser                     | newusergroup | md5   | aes     |

To delete SNMP user 'authuser', use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no snmp-server user authuser
```

**Related  
commands**    `show snmp-server user`  
                  `snmp-server view`

# snmp-server view

**Overview** Use this command to create an SNMP view that specifies a sub-tree of the MIB. Further sub-trees can then be added by specifying a new OID to an existing view. Views can be used in SNMP communities or groups to control the remote manager's access.

**NOTE:** *The object identifier must be specified in a sequence of integers separated by decimal points.*

The **no** variant of this command removes the specified view on the device. The view must already exist.

**Syntax** `snmp-server view <view-name> <mib-name> {included|excluded}`  
`no snmp-server view <view-name>`

| Parameter   | Description                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------|
| <view-name> | SNMP server view name.<br>The view name is a string up to 20 characters long and is case sensitive. |
| <mib-name>  | Object identifier of the MIB.                                                                       |
| included    | Include this OID in the view.                                                                       |
| excluded    | Exclude this OID in the view.                                                                       |

**Mode** Global Configuration

**Examples** The following command creates a view called "loc" that includes the system location MIB sub-tree.

```
awplus(config)# snmp-server view loc 1.3.6.1.2.1.1.6.0 included
```

To remove the view "loc" use the following command

```
awplus(config)# no snmp-server view loc
```

**Related commands** [show snmp-server view](#)  
[snmp-server community](#)

# test snmp trap snmp

**Overview** Use this command to test connectivity between the AlliedWare Plus device and an SNMP manager. The command tests the connectivity by sending a one-off coldStart or warmStart trap.

It does not matter whether you send a coldStart or warmStart trap; either trap lets you test the connectivity.

**Syntax** `test snmp trap snmp coldstart`  
`test snmp trap snmp warmstart`

| Parameter              | Description                                                                                                          |
|------------------------|----------------------------------------------------------------------------------------------------------------------|
| <code>coldstart</code> | Send a one-off coldStart trap. This trap indicates that the SNMP agent is restarting with a configuration change.    |
| <code>warmstart</code> | Send a one-off warmStart trap. This trap indicates that the SNMP agent is restarting without a configuration change. |

**Default** n/a

**Mode** Privileged Exec

**Example** To send a one-off coldStart trap to the SNMP manager configured on the device, use the command:

```
awplus# test snmp trap snmp coldstart
```

**Related commands** [snmp-server host](#)

**Command changes** Version 5.5.4-2.3: command added

# undebbug snmp

**Overview** This command applies the functionality of the no [debug snmp](#) command.

# 49

# Mail (SMTP) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure mail. The mail feature uses Simple Mail Transfer Protocol (SMTP) to transfer mail from an internal email client operating within the AlliedWare Plus device. This feature is typically used to email event notifications to an external email server from the AlliedWare Plus device.

For information on using the mail feature, see the [Mail \(SMTP\) Feature Overview and Configuration Guide](#).

- Command List**
- “[debug mail](#)” on page 2355
  - “[delete mail](#)” on page 2356
  - “[mail](#)” on page 2357
  - “[mail from](#)” on page 2359
  - “[mail smtpserver](#)” on page 2360
  - “[mail smtpserver authentication](#)” on page 2361
  - “[mail smtpserver port](#)” on page 2363
  - “[mail smtpserver tls](#)” on page 2365
  - “[show counter mail](#)” on page 2366
  - “[show mail](#)” on page 2367
  - “[undebbug mail](#)” on page 2368

# debug mail

**Overview** This command turns on debugging for sending emails.  
The **no** variant of this command turns off debugging for sending emails.

**Syntax** debug mail  
no debug mail

**Mode** Privileged Exec

**Examples** To turn on debugging for sending emails, use the command:  
awplus# debug mail  
To turn off debugging for sending emails, use the command:  
awplus# no debug mail

**Related commands** delete mail  
mail  
mail from  
mail smtpserver  
show counter mail  
show mail  
undebug mail

# delete mail

**Overview** This command deletes mail from the queue.

You need the *mail-id* from the **show mail** command output to delete specific emails, or use the **all** parameter to clear all messages in the queue completely.

**Syntax** `delete mail [mail-id <mail-id>|all]`

| Parameter | Description                                                                                                                    |
|-----------|--------------------------------------------------------------------------------------------------------------------------------|
| mail-id   | Deletes a single mail from the mail queue.                                                                                     |
|           | <i>&lt;mail-id&gt;</i> A unique mail ID number. Use the <a href="#">show mail</a> command to display this for an item of mail. |
| all       | Delete all the mail in the queue.                                                                                              |

**Mode** Privileged Exec

**Examples** To delete the unique mail item “20060912142356.1234” from the queue, use the command:

```
awplus# delete mail 20060912142356.1234
```

To delete all mail from the queue, use the command:

```
awplus# delete mail all
```

**Related commands**

- [debug mail](#)
- [mail](#)
- [mail from](#)
- [mail smtpserver](#)
- [show mail](#)



# mail

**Overview** This command sends an email using the SMTP protocol. If you specify a file the text inside the file is sent in the message body.

If you do not specify the **to**, **file**, or **subject** parameters, the CLI prompts you for the missing information.

Before you can send mail using this command, you must specify the sending email address using the [mail from](#) command and a mail server using the [mail smtpserver](#) command.

**Syntax** mail [to <to>] [subject <subject>] [file <filename>]

| Parameter | Description                                                                                      |
|-----------|--------------------------------------------------------------------------------------------------|
| to        | The email recipient.                                                                             |
|           | <to> Email address.                                                                              |
| subject   | Description of the subject of this email. Use quote marks when the subject text contains spaces. |
|           | <subject> String.                                                                                |
| file      | File to insert as text into the message body.                                                    |
|           | <filename> String.                                                                               |

**Mode** Privileged Exec

**Usage notes** When you use the **mail** command you can use parameter substitutions in the subject field. The following table lists the parameters that can be substituted and their descriptions:

| Parameter            | Description                                                                                                            |
|----------------------|------------------------------------------------------------------------------------------------------------------------|
| <%N>                 | When this parameter is specified, the %N is replaced by the host name of your device.                                  |
| <%S>                 | When this parameter is specified, the %S is replaced by the serial number of your device.                              |
| <%D><br><%L><br><%T> | When any of these parameters is specified, they are replaced by the current date and time (local time) on your device. |
| <%U>                 | When this parameter is specified, the %U is replaced by the current date and time (UTC time) on your device.           |

**NOTE:** If no local time is configured, it will use UTC.

**Examples** To send an email to "admin@example.com" with the subject "test email" and with the message body inserted from the file "test.conf", use the command:

```
awplus# mail to admin@example.com subject "test email" filename
test.conf
```

To send an email using parameter substitutions for the host name, serial number and date, use the commands:

```
awplus# mail to admin@example.com subject "Sending email from
Hostname:%N Serial Number:%S Date:%T"
```

**Related  
commands**

[debug mail](#)

[delete mail](#)

[mail from](#)

[mail smtpserver](#)

[mail smtpserver authentication](#)

[mail smtpserver port](#)

[show counter mail](#)

[show mail](#)

# mail from

**Overview** This command sets an email address as the sender. You must specify a sending email address with this command before you can send email.

Use the **no** variant of this command to remove the “mail from” address.

**Syntax** mail from <from>  
no mail from

| Parameter | Description                                                                |
|-----------|----------------------------------------------------------------------------|
| <from>    | The email address that the mail is sent from (also known as the hostname). |

**Mode** Global Configuration

**Example** To set up your email address as the sender “kaji@nerv.com”, use the command:

```
awplus(config)# mail from kaji@nerv.com
```

**Related commands**

- debug mail
- delete mail
- mail
- mail smtpserver
- show counter mail
- show mail
- undebug mail

# mail smtpserver

**Overview** This command specifies the IP address or domain name of the SMTP server that your device sends email to. You must specify a mail server with this command before you can send email.

Use the **no** variant of this command to remove the configured mail server.

**Syntax** mail smtpserver {<ip-address>|<name>}  
no mail smtpserver

| Parameter    | Description                                                           |
|--------------|-----------------------------------------------------------------------|
| <ip-address> | Internet Protocol (IP) address for the mail server.                   |
| <name>       | Domain name (FQDN) for the mail server (also known as the host name). |

**Mode** Global Configuration

**Usage notes** If you specify the server by specifying its domain name, you must also ensure that the DNS client on your device is enabled. It is enabled by default but if it has been disabled, you can re-enable it by using the [ip domain-lookup](#) command.

**Examples** To specify a mail server at "192.168.0.1", use the command:

```
awplus(config)# mail smtpserver 192.168.0.1
```

To specify a mail server that has a host name of "smtp.example.com", use the command:

```
awplus(config)# mail smtpserver smtp.example.com
```

To remove the configured mail server, use the command:

```
awplus(config)# no mail smtpserver
```

**Related commands**

- [debug mail](#)
- [delete mail](#)
- [mail](#)
- [mail from](#)
- [show counter mail](#)
- [show mail](#)

# mail smtpserver authentication

**Overview** Use this command to configure SMTP mail server authentication.

Use the **no** variant of this command to remove the configured SMTP mail server authentication.

**Syntax** `mail smtpserver authentication {crammd5|login|plain} username  
<username> password [8] <password>`  
`no mail smtpserver authentication`

| Parameter  | Description                                                                                                                                                                |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| crammd5    | This is a Challenge Request Authentication Mechanism based on the HMAC-MD5 mechanism and is the most secure option.                                                        |
| login      | A BASE64 encryption method                                                                                                                                                 |
| plain      | A BASE64 encryption method                                                                                                                                                 |
| <username> | Registered user name                                                                                                                                                       |
| 8          | The registered user password is presented in an already encrypted format. This is how the running configuration stores the plain text password and is not for general use. |
| <password> | Registered user password                                                                                                                                                   |

**Default** No authentication option is set by default.

**Mode** Global Configuration

**Usage notes** You cannot change the IP address or Domain Name of the SMTP server if authentication is configured. If you attempt to change it when authentication is configured, the following error message is displayed:

```
% Error: authentication configuration still exists
```

**Examples** To configure the SMTP mail server authentication to crammd5, use the commands:

```
awplus# configure terminal
awplus(config)# mail smtpserver authentication crammd5 username
admin password unguessablePassword
```

To remove SMTP mail server authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no mail smtpserver authentication
```

**Output** Figure 49-1: Example output from **show mail**:

```
awplus#show mail
Mail Settings

State : Alive
SMTP Server : 1.2.3.4
Host Name : admin@example.com
Authentication : crammd5
Username : admin
Debug : Disabled

awplus#show running-config
!
mail smtpserver authentication plain username admin password 8
aF0a9pkjbmXGfl6TlSk/GakeIK5tMYN6LqMYT8Ia2qw=
!
```

**Related commands**

- [debug mail](#)
- [delete mail](#)
- [mail](#)
- [mail from](#)
- [mail smtpserver](#)
- [mail smtpserver port](#)
- [show counter mail](#)
- [show mail](#)

**Command changes** Version 5.4.8-1.1: command added

# mail smtpserver port

**Overview** Use this command to configure the SMTP mail client/server communication port.

Use the **no** variant of this command to remove the configured port and set it back to the default port.

**Syntax** mail smtpserver port <port>  
no mail smtpserver port

| Parameter | Description                           |
|-----------|---------------------------------------|
| <port>    | Port number from the range 1 to 65535 |

**Default** The default port value is 25 if TLS is not enabled for the SMTP server, 587 if TLS is enabled with STARTTLS, and 465 if TLS is enabled with SMTPS.

**Mode** Global Configuration

**Examples** To configure the mail server communication over port 587, use the commands:

```
awplus# configure terminal
awplus(config)# mail smtpserver port 587
```

To revert to the default SMTP mail server communication port, use the commands:

```
awplus# configure terminal
awplus(config)# no mail smtpserver port
```

**Output** Figure 49-2: Example output from **show mail**:

```
awplus#show mail
Mail Settings

State : Alive
SMTP Server : 10.24.165.4
Host Name : admin@example.com
Authentication : plain
Username : admin
Port : 587
Use TLS : STARTTLS
Debug : Disabled

awplus#show running-config
!
mail smtpserver port 587
!
```

**Related commands** debug mail  
delete mail

mail  
mail from  
mail smtpserver  
mail smtpserver tls  
show counter mail  
show mail

**Command changes** Version 5.4.8-1.1: command added



# mail smtpserver tls

**Overview** Use this command to configure the device to send emails over a TLS connection to the SMTP server instead of sending in clear-text. If the SMTP server does not support receiving emails over a TLS connection, sending emails from the device will fail.

Use the **no** variant of this command to configure the device to send emails over an unencrypted TCP connection (clear text).

**Syntax** mail smtpserver tls [starttls|smtps]  
no mail smtpserver tls

| Parameter | Description                                                                                                                   |
|-----------|-------------------------------------------------------------------------------------------------------------------------------|
| starttls  | The connection starts as clear-text SMTP first and then the client establishes a TLS connection using the STARTTLS extension. |
| smtps     | Use a TLS connection from the start.                                                                                          |

**Default** By default, TLS is disabled and the device sends emails in clear-text.

**Mode** Global Configuration

**Examples** To send emails to the SMTP server over a TLS connection that will be established by the STARTTLS method, use the commands:

```
awplus# configure terminal
awplus(config)# mail smtpserver tls starttls
```

To send emails to the SMTP server over a TLS connection from the beginning, use the commands:

```
awplus# configure terminal
awplus(config)# mail smtpserver tls smtps
```

To send emails to the SMTP server in clear text, use the commands:

```
awplus# configure terminal
awplus(config)# no mail smtpserver tls
```

**Related commands** [mail](#)  
[show mail](#)  
[mail smtpserver](#)  
[mail smtpserver port](#)  
[mail smtpserver authentication](#)

**Command changes** Version 5.5.3-0.1: command added

# show counter mail

**Overview** This command displays the mail counters.

**Syntax** show counter mail

**Mode** User Exec and Privileged Exec

**Example** To show the emails in the queue use the command:

```
awplus# show counter mail
```

**Output** Figure 49-3: Example output from the **show counter mail** command

```
Mail Client (SMTP) counters
Mails Sent 2
Mails Sent Fails 1
```

**Table 1:** Parameters in the output of the **show counter mail** command

| Parameter        | Description                                                                   |
|------------------|-------------------------------------------------------------------------------|
| Mails Sent       | The number of emails sent successfully since the last device restart.         |
| Mails Sent Fails | The number of emails the device failed to send since the last device restart. |

**Related commands**

- [debug mail](#)
- [delete mail](#)
- [mail](#)
- [mail from](#)
- [show mail](#)

# show mail

**Overview** This command displays the emails in the queue.

**Syntax** show mail

**Mode** Privileged Exec

**Example** To display the emails in the queue use the command:

```
awplus# show mail
```

**Output** Figure 49-4: Example output from the **show mail** command:

```
awplus#show mail
Mail Settings

State : Alive
SMTP Server : example.net
Host Name : test@example.com
Authentication : login
Username : admin
Port : 587
Use TLS : STARTTLS
Debug : Disabled

Messages

There is no mail in the queue.
```

**Related commands**

- [delete mail](#)
- [mail](#)
- [mail from](#)
- [mail smtpserver](#)
- [mail smtpserver tls](#)
- [show counter mail](#)
- [mail smtpserver port](#)
- [undebug mail](#)

# undebug mail

**Overview** This command applies the functionality of the no [debug mail](#) command.

# 50

# RMON Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure Remote Monitoring (RMON).

For an introduction to RMON and an RMON configuration example, see the [RMON Feature Overview and Configuration Guide](#).

RMON is disabled by default in AlliedWare Plus™. No RMON alarms or events are configured.

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Command List**
- [“rmon alarm”](#) on page 2370
  - [“rmon collection history”](#) on page 2373
  - [“rmon collection stats”](#) on page 2374
  - [“rmon event”](#) on page 2375
  - [“show rmon alarm”](#) on page 2376
  - [“show rmon event”](#) on page 2377
  - [“show rmon history”](#) on page 2379
  - [“show rmon statistics”](#) on page 2381

# rmon alarm

**Overview** Use this command to configure an RMON alarm to monitor the value of an SNMP object, and to trigger specified events when the monitored object crosses specified thresholds.

To specify the action taken when the alarm is triggered, use the event index of an event defined by the [rmon event](#) command.

Use the **no** variant of this command to remove the alarm configuration.

**NOTE:** You can only configure alarms for Eth and tunnel interfaces.

## Syntax User-defined alarm:

```
rmon alarm <alarm-index> <oid.index> interval <1-2147483647>
{delta|absolute} rising-threshold <1-2147483647> event
<rising-event-index> falling-threshold <1-2147483647> event
<falling-event-index> [alarmstartup {1|2|3}] [owner <owner>]
```

## Eventwatch alarm, do not use (used by Vista Manager EX only):

```
rmon alarm <alarm-index> <oid.index> interval <1-4294967295>
{delta|absolute} rising-threshold <1-2147483647> event
eventwatch falling-threshold <1-2147483647> event eventwatch
[owner <owner>]
```

```
no rmon alarm <alarm-index>
```

| Parameter                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <alarm-index>              | Alarm entry index value from the range 1 to 65535 seconds.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <oid.index>                | The variable SNMP MIB Object Identifier (OID) name to be monitored, for either etherStats or etherHistory entries. The entries can be either of the following formats:<br>- etherStatsEntry.<field>.<stats-index> or etherHistoryEntry.<field>.<history-index>, or<br>- etherStatsFieldName.<stats-index> or etherHistoryFieldName.<history-index>.<br>To define the <stats-index>, use the <a href="#">rmon collection stats</a> command.<br>To define the <history-index>, use the <a href="#">rmon collection history</a> command. |
| interval<br><1-2147483647> | Polling interval in seconds from the range 1 to 2147483647.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| delta                      | The RMON MIB alarmSampleType: the change in the monitored MIB object value between the beginning and end of the polling interval.                                                                                                                                                                                                                                                                                                                                                                                                     |
| absolute                   | The RMON MIB alarmSampleType: the value of the monitored MIB object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

| Parameter                           | Description                                                                                                                                                                                                               |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rising-threshold<br><1-2147483647>  | Rising threshold value of the alarm entry in seconds from the range 1 to 2147483647.                                                                                                                                      |
| <rising-event-index>                | From the range 1 to 65535 seconds. The event to be triggered when the monitored object value reaches the rising threshold value. This is the event index of an event specified by the <a href="#">rmon event</a> command. |
| eventwatch                          | The alarm triggers an eventwatch event. This mechanism is used by Vista Manager EX, the Allied Telesis network management and monitoring tool. Do not use this parameter; use the <rising-event-index> parameter instead. |
| falling-threshold<br><1-2147483647> | Falling threshold value of the alarm entry in seconds from the range 1 to 2147483647.                                                                                                                                     |
| <falling-event-index>               | From the range 1 to 65535 seconds. The event to be triggered when the monitored object value reaches the falling threshold value. This is an event index of an event specified by the <a href="#">rmon event</a> command. |
| eventwatch                          | The alarm triggers an eventwatch event. This mechanism is used by Vista Manager EX, the Allied Telesis network management and monitoring tool. Do not use this parameter; use the <rising-event-index> parameter instead. |
| alarmstartup {1 2 3}                | Whether RMON can trigger a falling alarm (1), a rising alarm (2) or either (3) when you first start monitoring. See the Usage section for more information. The default is setting 3 (either).                            |
| owner <owner>                       | Arbitrary owner name to identify the alarm entry.                                                                                                                                                                         |

**Default** By default, there are no alarms.

**Mode** Global Configuration

**Usage notes** RMON alarms have a rising and falling threshold. Once the alarm monitoring is operating, you cannot have a falling alarm unless there has been a rising alarm and vice versa.

However, when you start RMON alarm monitoring, an alarm must be generated without the other type of alarm having first been triggered. The **alarmstartup** parameter allows this. It is used to say whether RMON can generate a rising alarm (1), a falling alarm (2) or either alarm (3) as the first alarm.

Note that you specify the SNMP MIB Object Identifier (OID) as a dotted decimal value, using one of the following forms:

- etherStatsEntry.<field>.<stats-index> or  
etherHistoryEntry.<field>.<history-index>.  
For example, etherHistoryEntry.8.8

- or, etherStatsFieldName.<stats-index> or etherHistoryFieldName.<history-index>. For example, etherHistoryMulticastPkts.8

If you enter the first form (etherHistoryEntry.8.8), the device will save it as the second form (etherHistoryMulticastPkts.8) in the running-config.

**Example** To configure an alarm to:

- monitor the change per minute in the etherStatsPkt value for interface 22 (defined by stats-index 22 in the [rmon collection stats](#) command)
- and trigger event 2 (defined by the [rmon event](#) command) when the change reaches the rising threshold 400
- and trigger event 3 when it reaches the falling threshold 200
- and identify this alarm as belonging to the user with username Maria

use the following commands:

```
awplus# configure terminal
awplus(config)# rmon alarm 229 etherStatsEntry.22.5 interval 60
delta rising-threshold 400 event 2 falling-threshold 200 event
3 alarmstartup 3 owner maria
```

To configure an alarm that:

- every 10 seconds, checks the number of multicast packets
- in the latest history control table entry controlled by history-index 8
- to see if the number of packets has increased to 15 or dropped to 5
- and if it has, triggers event 10

use either of the following commands:

```
awplus(config)# rmon alarm 56 etherHistoryMulticastPkts.8
interval 10 absolute rising-threshold 15 event 10
falling-threshold 5 event 10

awplus(config)# rmon alarm 56 etherHistoryEntry.8.8 interval 10
absolute rising-threshold 15 event 10 falling-threshold 5 event
10
```

**Related commands** [rmon collection history](#)  
[rmon collection stats](#)  
[rmon event](#)



# rmon collection history

**Overview** Use this command to create a history statistics control group to store a specified number of snapshots (buckets) of the standard RMON statistics for the switch port, and to collect these statistics at specified intervals. If there is sufficient memory available, then the device will allocate memory for storing the set of buckets that comprise this history control.

Use the **no** variant of this command to remove the specified history control configuration.

**NOTE:** A history can only be collected for tunnels, eth interfaces and switch port interfaces.

**Syntax** `rmon collection history <history-index> [buckets <1-65535>]  
[interval <1-3600>] [owner <owner>]  
no rmon collection history <history-index>`

| Parameter         | Description                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------|
| <history-index>   | A unique RMON history control entry index value from the range 1 to 65535.                           |
| buckets <1-65535> | Number of requested buckets to store snapshots from the range 1 to 65535. The default is 50 buckets. |
| interval <1-3600> | Polling interval in seconds. Default 1800 second polling interval from the range 1 to 3600.          |
| owner <owner>     | Owner name to identify the entry.                                                                    |

**Default** The default interval is 1800 seconds and the default number of buckets is 50.

**Mode** Interface Configuration

**Example** To create a history statistics control group with ID 200 to store 500 snapshots with an interval of 600 seconds, use the commands:

```
awplus# configure terminal
awplus(config-if)# rmon collection history 200 buckets 500
interval 600 owner herbert
```

To disable the history statistics control group, use the commands:

```
awplus# configure terminal
awplus(config-if)# no rmon collection history 200
```

**Related commands** [rmon alarm](#)  
[rmon collection stats](#)  
[rmon event](#)

# rmon collection stats

**Overview** Use this command to enable the collection of RMON statistics on a switch port, and assign an index number by which to access these collected statistics.

Use the **no** variant of this command to stop collecting RMON statistics on this switch port.

**NOTE:** Statistics can only be collected for tunnels, eth interfaces and switch port interfaces.

**Syntax** `rmon collection stats <collection-index> [owner <owner>]`  
`no rmon collection stats <collection-index>`

| Parameter          | Description                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <collection-index> | Give this collection of statistics an index number to uniquely identify it. This is the index to use to access the statistics collected for this switch port. Use a number in the range of 1 to 65535. |
| owner <owner>      | An arbitrary owner name to identify this statistics collection entry.                                                                                                                                  |

**Default** RMON statistics are not enabled by default.

**Mode** Interface Configuration

**Example** To enable the collection of RMON statistics with a statistics index of 200, use the commands:

```
awplus# configure terminal
awplus(config-if)# rmon collection stats 200 owner myrtle
```

To stop collecting RMON statistics, use the commands:

```
awplus# configure terminal
awplus(config-if)# no rmon collection stats 200
```

**Related commands** [rmon alarm](#)  
[rmon collection history](#)  
[rmon event](#)

# rmon event

**Overview** Use this command to create an event definition for a log or a trap or both. Then you can use this event index in the [rmon alarm](#) command to indicate whether to send an SNMP trap or log message (or both) when an alarm is triggered.

Use the **no** variant of this command to remove the event definition.

**Syntax**

```
rmon event <event-index> [description <description>|owner <owner>| trap <trap>]
```

```
rmon event <event-index> [log [description <description>|owner <owner>|trap <trap>]]
```

```
rmon event <event-index> [log trap [description <description>|owner <owner>]]
```

```
no rmon event <event-index>
```

| Parameter                | Description                               |
|--------------------------|-------------------------------------------|
| <event-index>            | <1-65535> Unique event entry index value. |
| log                      | Log event type.                           |
| trap                     | Trap event type.                          |
| log trap                 | Log and trap event type.                  |
| description<description> | Event entry description.                  |
| owner <owner>            | Owner name to identify the entry.         |

**Default** No event is configured by default.

**Mode** Global Configuration

**Example** To create an event definition with an index of 299 for a log, use this command:

```
awplus# configure terminal
awplus(config)# rmon event 299 log description cond3 owner
alfred
```

To remove the event definition, use the command:

```
awplus# configure terminal
awplus(config)# no rmon event 299
```

**Related commands** [rmon alarm](#)

# show rmon alarm

**Overview** Use this command to display the alarms and threshold configured for the RMON probe.

**Syntax** `show rmon alarm`

**Mode** User Exec and Privileged Exec

**Example** To display the alarms and threshold, use this command:

```
awplus# show rmon alarm
```

**Related commands** [rmon alarm](#)

# show rmon event

**Overview** Use this command to display the events configured for the RMON probe.

**Syntax** show rmon event

**Mode** User Exec and Privileged Exec

**Output** Figure 50-1: Example output from the **show rmon event** command

```
awplus#sh rmon event
event Index = 787
 Description TRAP
 Event type log & trap
 Event community name gopher
 Last Time Sent = 0
 Owner RMON_SNMP

event Index = 990
 Description TRAP
 Event type trap
 Event community name teabo
 Last Time Sent = 0
 Owner RMON_SNMP
```

**NOTE:** The following etherStats counters are not currently available for Layer 3 interfaces:

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

**Example** To display the events configured for the RMON probe, use this command:

```
awplus# show rmon event
```

**Related  
commands** [rmon event](#)

# show rmon history

**Overview** Use this command to display the parameters specified on all the currently defined RMON history collections on the device.

**Syntax** `show rmon history`

**Mode** User Exec and Privileged Exec

**Output** Figure 50-2: Example output from the **show rmon history** command

```
awplus#sh rmon history
history index = 56
 data source ifindex = 4501
 buckets requested = 34
 buckets granted = 34
 Interval = 2000
 Owner Andrew

history index = 458
 data source ifindex = 5004
 buckets requested = 400
 buckets granted = 400
 Interval = 1500
 Owner trev
=====
```

**NOTE:** The following *etherStats* counters are not currently available for Layer 3 interfaces:

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

**Example** To display the parameters specified on all the currently defined RMON history collections, use the commands:

```
awplus# show rmon history
```

**Related commands** [rmon collection history](#)



# show rmon statistics

**Overview** Use this command to display the current values of the statistics for all the RMON statistics collections currently defined on the device.

**Syntax** `show rmon statistics`

**Mode** User Exec and Privileged Exec

**Example** To display the current values of the statistics for all the RMON statistics collections, use the commands:

```
awplus# show rmon statistics
```

**Output** Figure 50-3: Example output from the **show rmon statistics** command

```
awplus#show rmon statistics
rmon collection index 45
stats->ifindex = 4501
input packets 1279340, bytes 85858960, dropped 00, multicast packets 1272100
output packets 7306090, bytes 268724, multicast packets 7305660 broadcast
packets 290
rmon collection index 679
stats->ifindex = 5013
input packets 00, bytes 00, dropped 00, multicast packets 00
output packets 8554550, bytes 26777324, multicast packets 8546690 broadcast
packets 7720
```

**NOTE:** The following etherStats counters are not currently available for Layer 3 interfaces:

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

**Related  
commands** [rmon collection stats](#)

# 51

# Secure Shell (SSH) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure Secure Shell (SSH). For more information, see the [SSH Feature Overview and Configuration Guide](#).

- Command List**
- “[banner login \(SSH\)](#)” on page 2385
  - “[clear ssh](#)” on page 2386
  - “[crypto key destroy hostkey](#)” on page 2387
  - “[crypto key destroy userkey](#)” on page 2388
  - “[crypto key generate hostkey](#)” on page 2389
  - “[crypto key generate userkey](#)” on page 2391
  - “[crypto key pubkey-chain knownhosts](#)” on page 2393
  - “[crypto key pubkey-chain userkey](#)” on page 2395
  - “[debug ssh client](#)” on page 2397
  - “[debug ssh server](#)” on page 2398
  - “[service ssh](#)” on page 2399
  - “[show banner login](#)” on page 2401
  - “[show crypto key hostkey](#)” on page 2402
  - “[show crypto key pubkey-chain knownhosts](#)” on page 2404
  - “[show crypto key pubkey-chain userkey](#)” on page 2406
  - “[show crypto key userkey](#)” on page 2407
  - “[show running-config ssh](#)” on page 2408
  - “[show ssh](#)” on page 2410
  - “[show ssh client](#)” on page 2412

- ["show ssh server"](#) on page 2413
- ["show ssh server allow-users"](#) on page 2415
- ["show ssh server deny-users"](#) on page 2416
- ["ssh"](#) on page 2417
- ["ssh client"](#) on page 2419
- ["ssh client allow-legacy-ssh-rsa"](#) on page 2421
- ["ssh server"](#) on page 2422
- ["ssh server allow-legacy-ssh-rsa"](#) on page 2424
- ["ssh server allow-users"](#) on page 2425
- ["ssh server authentication"](#) on page 2427
- ["ssh server deny-users"](#) on page 2429
- ["ssh server max-auth-tries"](#) on page 2431
- ["ssh server resolve-host"](#) on page 2432
- ["ssh server scp"](#) on page 2433
- ["ssh server secure-algs"](#) on page 2434
- ["ssh server secure-ciphers"](#) on page 2435
- ["ssh server secure-hostkey"](#) on page 2436
- ["ssh server secure-kex"](#) on page 2437
- ["ssh server secure-mac"](#) on page 2438
- ["ssh server sftp"](#) on page 2439
- ["ssh server tcpforwarding"](#) on page 2440
- ["undebg ssh client"](#) on page 2441
- ["undebg ssh server"](#) on page 2442

# banner login (SSH)

**Overview** This command configures a login banner on the SSH server. This displays a message on the remote terminal of the SSH client before the login prompt. SSH client version 1 does not support this banner.

To add a banner, first enter the command **banner login**, and hit [Enter]. Write your message. You can use any character and spaces. Use Ctrl+D at the end of your message to save the text and re-enter the normal command line mode.

The banner message is preserved if the device restarts.

The **no** variant of this command deletes the login banner from the device.

**Syntax** banner login  
no banner login

**Default** No banner is defined by default.

**Mode** Global Configuration

**Examples** To set a login banner message, use the commands:

```
awplus# configure terminal
awplus(config)# banner login
```

The screen will prompt you to enter the message:

Type CNTL/D to finish.

... banner message comes here ...

Enter the message. Use Ctrl+D to finish, like this:

```
^D
awplus(config)#
```

To remove the login banner message, use the commands:

```
awplus# configure terminal
awplus(config)# no banner login
```

**Related commands** [show banner login](#)

# clear ssh

**Overview** This command deletes Secure Shell sessions currently active on the device. This includes both incoming and outgoing sessions. The deleted sessions are closed. You can only delete an SSH session if you are a system manager or the user who initiated the session. If **all** is specified then all active SSH sessions are deleted.

**Syntax** `clear ssh {<1-65535>|all}`

| Parameters | Description                                                                |
|------------|----------------------------------------------------------------------------|
| <1-65535>  | Specify a session ID in the range 1 to 65535 to delete a specific session. |
| all        | Delete all SSH sessions.                                                   |

**Mode** Privileged Exec

**Examples** To stop the current SSH session 123, use the command:

```
awplus# clear ssh 123
```

To stop all SSH sessions active on the device, use the command:

```
awplus# clear ssh all
```

**Related commands** [service ssh](#)  
[ssh](#)

# crypto key destroy hostkey

**Overview** This command deletes the existing public and private keys of the SSH server.

**Syntax** `crypto key destroy hostkey {dsa|ecdsa|ed25519|rsa|rsa1}`

| Parameters | Description                                                                                                                                                                          |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dsa        | Deletes the existing DSA public and private keys.                                                                                                                                    |
| ecdsa      | Deletes the existing ECDSA public and private keys.                                                                                                                                  |
| ed25519    | Deletes the existing Ed25519 public and private keys.                                                                                                                                |
| rsa        | Deletes the existing RSA public and private keys that were configured for SSH version 2 connections.                                                                                 |
| rsa1       | Deletes the existing RSA public and private keys that were configured for SSH version 1 connections. From AlliedWare Plus version 5.5.1-1.1 onwards, SSH version 1 is not supported. |

**Mode** Global Configuration

**Example** To destroy the RSA host key used for SSH version 2 connections, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy hostkey rsa
```

**Related commands** [crypto key generate hostkey](#)  
[service ssh](#)

**Command changes** Version 5.5.2-2.1: **ed25519** parameter added

# crypto key destroy userkey

**Overview** This command destroys the existing public and private keys of an SSH user configured on the device.

**Syntax** `crypto key destroy userkey <username>  
{dsa|ecdsa|ed25519|rsa|rsa1}`

| Parameters | Description                                                                                                                                                                            |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username> | Name of the user whose userkey you are destroying. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. |
| dsa        | Deletes the existing DSA userkey.                                                                                                                                                      |
| ecdsa      | Deletes the existing ECDSA userkey.                                                                                                                                                    |
| ed25519    | Deletes the existing Ed25519 userkey.                                                                                                                                                  |
| rsa        | Deletes the existing RSA userkey that was configured for SSH version 2 connections.                                                                                                    |
| rsa1       | Deletes the existing RSA userkey that was configured for SSH version 1 connections. From AlliedWare Plus version 5.5.1-1.1 onwards, SSH version 1 is not supported.                    |

**Mode** Global Configuration

**Example** To destroy the RSA user key for the SSH user `remoteuser`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy userkey remoteuser rsa
```

**Related commands**

- [crypto key generate hostkey](#)
- [crypto key generate userkey](#)
- [show ssh](#)
- [show crypto key hostkey](#)

**Command changes** Version 5.5.2-2.1: **ed25519** parameter added



# crypto key generate hostkey

**Overview** This command generates public and private keys for the SSH server.

When you enable the SSH server, if no host keys exist, the server automatically generates SSHv2 host key pairs using Ed25519 with a keysize of 256, ECDSA with a curve length of 384, and RSA with a 2048-bit key.

If you need a key with different parameters than this, you can use this command to generate that key before you enable the SSH server. If a host key exists with the same cryptography algorithm, this command replaces the old host key with the new key.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

**Syntax**

```
crypto key generate hostkey rsa [<1024-16384>]
crypto key generate hostkey ecdsa [<256|384|521>]
crypto key generate hostkey ed25519
```

| Parameters    | Description                                       |
|---------------|---------------------------------------------------|
| rsa           | Creates an RSA hostkey.                           |
| ecdsa         | Creates an ECDSA hostkey.                         |
| ed25519       | Creates an Ed25519 hostkey with a keysize of 256. |
| <1024-16384>  | The length in bits of the generated key.          |
| <256 384 521> | The ECDSA key size in bits.                       |

**Default** The default key length for RSA is 2048 bits.  
The default key size for ECDSA is 384 bits.

**Mode** Global Configuration

**Examples** To generate an RSA host key that is 4096 bits in length, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 4096
```

To generate an ECDSA host key with an elliptic curve size of 521 bits, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey ecdsa 521
```

To generate an Ed25519 host key with a keysize of 256, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey ed25519
```

**Related commands** `crypto key destroy hostkey`  
`service ssh`  
`show crypto key hostkey`

**Command changes** Version 5.5.2-2.1: **ed25519** parameter added  
Version 5.5.2-0.1: changes to key length and key size ranges and defaults  
Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

# crypto key generate userkey

**Overview** This command generates public and private keys for an SSH user using an RSA, ECDSA, or ED25519 cryptography algorithm. To use public key authentication, copy the public key of the user onto the remote SSH server.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

**Syntax** `crypto key generate userkey <username> rsa [<1024-16384>]`  
`crypto key generate userkey <username> ecdsa [<256|384|521>]`  
`crypto key generate userkey <username> ed25519`

| Parameters    | Description                                                                                                                                                                              |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username>    | Name of the user that the user key is generated for. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. |
| rsa           | Creates an RSA userkey.                                                                                                                                                                  |
| ecdsa         | Creates an ECDSA userkey.                                                                                                                                                                |
| ed25519       | Creates an Ed25519 userkey with a keysize of 256.                                                                                                                                        |
| <1024-16384>  | The length in bits of the generated key. The default is 2048 bits.                                                                                                                       |
| <256 384 521> | The ECDSA key size in bits. The default is 384.                                                                                                                                          |

**Default** The default key length for RSA is 2048 bits.  
The default key size for ECDSA is 384 bits.

**Mode** Global Configuration

**Examples** To generate a 4096-bit RSA user key for SSH version 2 connections for the user 'bob', use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey bob rsa 4096
```

To generate an ECDSA user key of key size 521 for the user 'lapo', use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo ecdsa 521
```

To generate an Ed25519 user key of key size 256 for the user 'lapo', use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo ed25519
```

**Related commands** [crypto key pubkey-chain userkey](#)  
[show crypto key userkey](#)

**Command changes** Version 5.5.2-2.1: **ed25519** parameter added  
Version 5.5.2-0.1: changes to key length and key size ranges and defaults  
Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

# crypto key pubkey-chain knownhosts

**Overview** This command adds a public key of the specified SSH server to the known host database on your device. The SSH client on your device uses this public key to verify the remote SSH server.

The key is retrieved from the server. Before adding a key to this database, check that the key sent to you is correct.

If the server's key changes, or if your SSH client does not have the public key of the remote SSH server, then your SSH client will inform you that the public key of the server is unknown or altered.

The **no** variant of this command deletes the public key of the specified SSH server from the known host database on your device.

**Syntax** `crypto key pubkey-chain knownhosts [ip|ipv6] <hostname>  
[ecdsa|rsa]  
no crypto key pubkey-chain knownhosts <1-65535>`

| Parameter  | Description                                                                                                                                |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| ip         | Keyword used prior to specifying an IPv4 address                                                                                           |
| ipv6       | Keyword used prior to specifying an IPv6 address                                                                                           |
| <hostname> | IPv4/IPv6 address or hostname of a remote server in the format a.b.c.d for an IPv4 address, or in the format x:x::x:x for an IPv6 address. |
| ecdsa      | Specify the ECDSA public key of the server to be added to the known host database.                                                         |
| rsa        | Specify the RSA public key of the server to be added to the known host database.                                                           |
| <1-65535>  | Specify a key identifier when removing a key using the <b>no</b> parameter.                                                                |

**Default** If no cryptography algorithm is specified, then **rsa** is used as the default cryptography algorithm.

**Mode** Privilege Exec

**Usage notes** This command adds a public key of the specified SSH server to the known host database on the device. The key is retrieved from the server. The remote SSH server is verified by using this public key. The user is requested to check the key is correct before adding it to the database.

If the remote server's host key is changed, or if the device does not have the public key of the remote server, then SSH clients will inform the user that the public key of the server is altered or unknown.

**Examples** To add the RSA host key of the remote SSH host IPv4 address 192.0.2.11 to the known host database, use the command:

```
awplus# crypto key pubkey-chain knownhosts 192.0.2.11
```

To delete the second entry in the known host database, use the command:

```
awplus# no crypto key pubkey-chain knownhosts 2
```

**Validation Commands** [show crypto key pubkey-chain knownhosts](#)

**Command changes** Version 5.4.6-2.1: VRF-lite support added.

# crypto key pubkey-chain userkey

**Overview** This command adds a public key for an SSH user on the SSH server. This allows the SSH server to support public key authentication for the SSH user. When configured, the SSH user can access the SSH server without providing a password from the remote host.

The **no** variant of this command removes a public key for the specified SSH user that has been added to the public key chain. When a SSH user's public key is removed, the SSH user can no longer login using public key authentication.

**Syntax** `crypto key pubkey-chain userkey <username> [<filename>]`  
`no crypto key pubkey-chain userkey <username> <1-65535>`

| Parameters | Description                                                                                                                                                                                                           |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username> | Name of the user that the SSH server associates the key with. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. Default: no default |
| <filename> | Filename of a key saved in flash. Valid characters are any printable character. You can add a key as a hexadecimal string directly into the terminal if you do not specify a filename.                                |
| <1-65535>  | The key ID number of the user's key. Specify the key ID to delete a key.                                                                                                                                              |

**Mode** Global Configuration

**Usage notes** You should import the public key file from the client node. The device can read the data from a file on the flash or user terminal.

Or you can add a key as text into the terminal. To add a key as text into the terminal, first enter the command **crypto key pubkey-chain userkey <username>**, and hit [Enter]. Enter the key as text. Note that the key you enter as text must be a valid SSH RSA key, not random ASCII text. Use [Ctrl]+D after entering it to save the text and re-enter the normal command line mode.

Note you can generate a valid SSH RSA key on the device first using the **crypto key generate host rsa** command. View the SSH RSA key generated on the device using the **show crypto hostkey rsa** command. Copy and paste the displayed SSH RSA key after entering the **crypto key pubkey-chain userkey <username>** command. Use [Ctrl]+D after entering it to save it.

**Examples** To generate a valid SSH RSA key on the device and add the key, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto key generate host rsa
awplus(config)# exit

awplus# show crypto key hostkey
rsaAAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fcOw1TStpb9J20bWlunUC768EoWhyPW6FZ2t5360O5M29EpKBmGqlkQaz5V0mU9IQe66+5YyD4UxOKSDtTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/pqGDijj4SvfZZfeITzvvyZW4/I4pbN8=

awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey joeType CNTRL/D
to
finish:AAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fcOw1TStpb9J20bWlunUC768EoWhyPW6FZ2t5360O5M29EpKBmGqlkQaz5V0mU9IQe66+5YyD4UxOKSDtTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/pqGDijj4SvfZZfeITzvvyZW4/I4pbN8=control-D

awplus(config)#
```

To add a public key for the user `graydon` from the file `key.pub`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey graydon key.pub
```

To add a public key for the user `tamara` from the terminal, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey tamara
```

and enter the key. Use Ctrl+D to finish.

To remove the first key entry from the public key chain of the user `john`, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto key pubkey-chain userkey john 1
```

**Related commands** [show crypto key pubkey-chain userkey](#)



# debug ssh client

**Overview** This command enables the SSH client debugging facility. When enabled, any SSH, SCP and SFTP client sessions send diagnostic messages to the login terminal.

The **no** variant of this command disables the SSH client debugging facility. This stops the SSH client from generating diagnostic debugging message.

**Syntax** `debug ssh client [brief|full]`  
`no debug ssh client`

| Parameter | Description               |
|-----------|---------------------------|
| brief     | Enables brief debug mode. |
| full      | Enables full debug mode.  |

**Default** SSH client debugging is disabled by default.

**Mode** Privileged Exec and Global Configuration

**Examples** To start SSH client debugging, use the command:

```
awplus# debug ssh client
```

To start SSH client debugging with extended output, use the command:

```
awplus# debug ssh client full
```

To disable SSH client debugging, use the command:

```
awplus# no debug ssh client
```

**Related commands** [debug ssh server](#)  
[show ssh client](#)  
[undebug ssh client](#)

**Command changes** Version 5.5.3-1.1: added to AR1050V

# debug ssh server

**Overview** This command enables the SSH server debugging facility. When enabled, the SSH server sends diagnostic messages to the system log. To display the debugging messages on the terminal, use the **terminal monitor** command.

The **no** variant of this command disables the SSH server debugging facility. This stops the SSH server from generating diagnostic debugging messages.

**Syntax** `debug ssh server [brief|full]`  
`no debug ssh server`

| Parameter | Description               |
|-----------|---------------------------|
| brief     | Enables brief debug mode. |
| full      | Enables full debug mode.  |

**Default** SSH server debugging is disabled by default.

**Mode** Privileged Exec and Global Configuration

**Examples** To start SSH server debugging, use the command:

```
awplus# debug ssh server
```

To start SSH server debugging with extended output, use the command:

```
awplus# debug ssh server full
```

To disable SSH server debugging, use the command:

```
awplus# no debug ssh server
```

**Related commands** [debug ssh client](#)  
[show ssh server](#)  
[undebug ssh server](#)

# service ssh

**Overview** Use this command to enable the Secure Shell server on the device. Once enabled, connections coming from SSH clients are accepted.

When you enable the SSH server, if no host keys exist, the server automatically generates SSHv2 host key pairs using ECDSA with a curve length of 384, and RSA with a 1024-bit key.

If you need a key with different parameters than this, you can use the [crypto key generate hostkey](#) command to generate that key before you enable the SSH server.

Use the **no** variant of this command to disable the Secure Shell server. When the Secure Shell server is disabled, connections from SSH, SCP, and SFTP clients are not accepted. This command does not affect existing SSH sessions. To terminate existing sessions, use the [clear ssh](#) command.

**Syntax** `service ssh [ip|ipv6]`  
`no service ssh [ip|ipv6]`

**Default** The Secure Shell server is disabled by default. Both IPv4 and IPv6 Secure Shell server are enabled when you issue **service ssh** without specifying the optional **ip** or **ipv6** parameters.

**Mode** Global Configuration

**Examples** To enable both the IPv4 and the IPv6 Secure Shell server, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh
```

To enable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ip
```

To enable the IPv6 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ipv6
```

To disable both the IPv4 and the IPv6 Secure Shell server, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh
```

To disable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ip
```

To disable the IPv6 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ipv6
```

**Related  
commands**

[crypto key generate hostkey](#)  
[show running-config ssh](#)  
[show ssh server](#)  
[ssh server allow-users](#)  
[ssh server deny-users](#)

**Command  
changes**

Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

# show banner login

**Overview** This command displays the banner message configured on the device. The banner message is displayed to the remote user before user authentication starts.

**Syntax** `show banner login`

**Mode** User Exec, Privileged Exec, Global Configuration, Interface Configuration, Line Configuration

**Example** To display the current login banner message, use the command:

```
awplus# show banner login
```

**Related commands** [banner login \(SSH\)](#)

# show crypto key hostkey

**Overview** This command displays the public keys generated on the device for the SSH server.

When you enable the SSH server, if no host keys exist, the server automatically generates SSHv2 host key pairs using ECDSA with a curve length of 384, and RSA with a 1024-bit key.

The private key remains on the device secretly. The public key is copied to SSH clients to identify the server. This command displays the public key.

**Syntax** `show crypto key hostkey [dsa|ecdsa|rsa|rsa1]`

| Parameter | Description                                                                                                                                  |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------|
| dsa       | Displays the DSA algorithm public key.                                                                                                       |
| ecdsa     | Displays the ECDSA algorithm public key.                                                                                                     |
| rsa       | Displays the RSA algorithm public key for SSH version 2 connections.                                                                         |
| rsa1      | Displays the RSA algorithm public key for SSH version 1 connections. From AlliedWare Plus 5.5.1-1.1 onwards, SSH version 1 is not supported. |

**Mode** User Exec, Privileged Exec and Global Configuration

**Examples** To show the public keys generated on the device for SSH server, use the command:

```
awplus# show crypto key hostkey
```

To display the RSA public key of the SSH server, use the command:

```
awplus# show crypto key hostkey rsa
```

**Output** Figure 51-1: Example output from the **show crypto key hostkey** command

| Type  | Bits | Fingerprint                                        |
|-------|------|----------------------------------------------------|
| rsa   | 1024 | SHA256:T/sVz5OoA1HHXcov9dXzGGQg8avRUYh1psxNSUcSOvs |
| ecdsa | 384  | SHA256:qVn/KpN5X5ct5CJakxE4OmPWmPvW2vIbBjF4SA2bZkM |

**Table 1:** Parameters in output of the **show crypto key hostkey** command

| Parameter   | Description                         |
|-------------|-------------------------------------|
| Type        | Algorithm used to generate the key. |
| Bits        | Length in bits of the key.          |
| Fingerprint | Checksum value for the public key.  |

**Related  
commands**   [crypto key destroy hostkey](#)  
                  [crypto key generate hostkey](#)

# show crypto key pubkey-chain knownhosts

**Overview** This command displays the list of public keys maintained in the known host database on the device.

**Syntax** show crypto key pubkey-chain knownhosts [<1-65535>]

| Parameter | Description                                                                           |
|-----------|---------------------------------------------------------------------------------------|
| <1-65535> | Key identifier for a specific key. Displays the public key of the entry if specified. |

**Default** Display all keys.

**Mode** User Exec, Privileged Exec and Global Configuration

**Examples** To display public keys of known SSH servers, use the command:

```
awplus# show crypto key pubkey-chain knownhosts
```

To display the key data of the first entry in the known host data, use the command:

```
awplus# show crypto key pubkey-chain knownhosts 1
```

**Output** Figure 51-2: Example output from the **show crypto key public-chain knownhosts** command

| No | Hostname                                 | Type | Fingerprint                                     |
|----|------------------------------------------|------|-------------------------------------------------|
| 1  | 172.16.23.1                              | rsa  | c8:33:b1:fe:6f:d3:8c:81:4e:f7:2a:aa:a5:be:df:18 |
| 2  | 172.16.23.10                             | rsa  | c4:79:86:65:ee:a0:1d:a5:6a:e8:fd:1d:d3:4e:37:bd |
| 3  | 5ffe:1053:ac21:ff00:0101:bcd:f:ffff:0001 | rsa1 | af:4e:b4:a2:26:24:6d:65:20:32:d9:6f:32:06:ba:57 |

**Table 2:** Parameters in the output of the **show crypto key public-chain knownhosts** command

| Parameter   | Description                             |
|-------------|-----------------------------------------|
| No          | Number ID of the key.                   |
| Hostname    | Host name of the known SSH server.      |
| Type        | The algorithm used to generate the key. |
| Fingerprint | Checksum value for the public key.      |

**Related commands** [crypto key pubkey-chain knownhosts](#)



**Command  
changes**

Version 5.5.3-1.1: added to AR1050V

Version 5.4.6-2.1: VRF-lite support added for AR-Series devices

# show crypto key pubkey-chain userkey

**Overview** This command displays the public keys registered with the SSH server for SSH users. These keys allow remote users to access the device using public key authentication. By using public key authentication, users can access the SSH server without providing password.

**Syntax** `show crypto key pubkey-chain userkey <username> [<1-65535>]`

| Parameter  | Description                                                                                                                                                                                          |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username> | User name of the remote SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. |
| <1-65535>  | Key identifier for a specific key.                                                                                                                                                                   |

**Default** Display all keys.

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the public keys for the user `manager` that are registered with the SSH server, use the command:

```
awplus# show crypto key pubkey-chain userkey manager
```

**Output** Figure 51-3: Example output from the **show crypto key public-chain userkey** command

| No | Type | Bits | Fingerprint                                     |
|----|------|------|-------------------------------------------------|
| 1  | dsa  | 1024 | 2b:cc:df:a8:f8:2e:8f:a4:a5:4f:32:ea:67:29:78:fd |
| 2  | rsa  | 2048 | 6a:ba:22:84:c1:26:42:57:2c:d7:85:c8:06:32:49:0e |

**Table 3:** Parameters in the output of the **show crypto key userkey** command

| Parameter   | Description                             |
|-------------|-----------------------------------------|
| No          | Number ID of the key.                   |
| Type        | The algorithm used to generate the key. |
| Bits        | Length in bits of the key.              |
| Fingerprint | Checksum value for the key.             |

**Related commands** [crypto key pubkey-chain userkey](#)

# show crypto key userkey

**Overview** This command displays the public keys created on this device for the specified SSH user.

**Syntax** `show crypto key userkey <username> [dsa|rsa|rsa1]`

| Parameter  | Description                                                                                                                                                                                         |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <username> | User name of the local SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. |
| dsa        | Displays the DSA public key.                                                                                                                                                                        |
| rsa        | Displays the RSA public key used for SSH version 2 connections.                                                                                                                                     |
| rsa1       | Displays the RSA key used for SSH version 1 connections.                                                                                                                                            |

**Mode** User Exec, Privileged Exec and Global Configuration

**Examples** To show the public key generated for the user, use the command:

```
awplus# show crypto key userkey manager
```

To store the RSA public key generated for the user manager to the file "user.pub", use the command:

```
awplus# show crypto key userkey manager rsa > manager-rsa.pub
```

**Output** Figure 51-4: Example output from the **show crypto key userkey** command

| Type | Bits | Fingerprint                                     |
|------|------|-------------------------------------------------|
| rsa  | 2048 | e8:d6:1b:c0:f4:b6:e6:7d:02:2e:a9:d4:a1:ca:3b:11 |
| rsa1 | 1024 | 12:25:60:95:64:08:8e:a1:8c:3c:45:1b:44:b9:33:9b |

**Table 4:** Parameters in the output of the **show crypto key userkey** command

| Parameter   | Description                             |
|-------------|-----------------------------------------|
| Type        | The algorithm used to generate the key. |
| Bits        | Length in bits of the key.              |
| Fingerprint | Checksum value for the key.             |

**Related commands** [crypto key generate userkey](#)

# show running-config ssh

**Overview** This command displays the current running configuration of Secure Shell (SSH).

**Syntax** show running-config ssh

**Mode** Privileged Exec and Global Configuration

**Example** To display the current configuration of SSH, use the command:

```
awplus# show running-config ssh
```

**Output** Figure 51-5: Example output from the **show running-config ssh** command

```
!
ssh server session-timeout 600
ssh server login-timeout 30
ssh server allow-users manager 192.168.1.*
ssh server allow-users john
ssh server deny-user john*.a-company.com
ssh server
```

**Table 5:** Parameters in the output of the **show running-config ssh** command

| Parameter                              | Description                                                                 |
|----------------------------------------|-----------------------------------------------------------------------------|
| ssh server                             | SSH server is enabled.                                                      |
| ssh server v2                          | SSH server is enabled and only support SSHv2.                               |
| ssh server<port>                       | SSH server is enabled and listening on the specified TCP port.              |
| no ssh server scp                      | SCP service is disabled.                                                    |
| no ssh server sftp                     | SFTP service is disabled.                                                   |
| ssh server session-timeout             | Configure the server session timeout.                                       |
| ssh server login-timeout               | Configure the server login timeout.                                         |
| ssh server max-startups                | Configure the maximum number of concurrent sessions waiting authentication. |
| no ssh server authentication password  | Password authentication is disabled.                                        |
| no ssh server authentication publickey | Public key authentication is disabled.                                      |

**Table 5:** Parameters in the output of the **show running-config ssh** command

| Parameter              | Description                                    |
|------------------------|------------------------------------------------|
| ssh server allow-users | Add the user (and hostname) to the allow list. |
| ssh server deny-users  | Add the user (and hostname) to the deny list.  |

**Related  
commands**   [service ssh](#)  
                  [show ssh server](#)

# show ssh

**Overview** This command displays the active SSH sessions on the device, both incoming and outgoing.

**Syntax** show ssh

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the current SSH sessions on the device, use the command:

```
awplus# show ssh
```

**Output** Figure 51-6: Example output from the **show ssh** command

| Secure Shell Sessions: |      |        |                                         |          |           |             |  |
|------------------------|------|--------|-----------------------------------------|----------|-----------|-------------|--|
| ID                     | Type | Mode   | Peer Host                               | Username | State     | Filename    |  |
| 414                    | ssh  | server | 172.16.23.1                             | root     | open      |             |  |
| 456                    | ssh  | client | 172.16.23.10                            | manager  | user-auth |             |  |
| 459                    | scp  | client | 172.16.23.12                            | root     | download  | example.awd |  |
| 463                    | ssh  | client | 5ffe:33fe:5632:ffbb:bc35:ddee:0101:ac51 | manager  | user-auth |             |  |

**Table 6:** Parameters in the output of the **show ssh** command

| Parameter | Description                                                                                              |
|-----------|----------------------------------------------------------------------------------------------------------|
| ID        | Unique identifier for each SSH session.                                                                  |
| Type      | Session type; either SSH, SCP, or SFTP.                                                                  |
| Mode      | Whether the device is acting as an SSH client (client) or SSH server (server) for the specified session. |
| Peer Host | The hostname or IP address of the remote server or client.                                               |
| Username  | Login user name of the server.                                                                           |

**Table 6:** Parameters in the output of the **show ssh** command (cont.)

| Parameter | Description                                                           |                                                 |
|-----------|-----------------------------------------------------------------------|-------------------------------------------------|
| State     | The current state of the SSH session. One of:                         |                                                 |
|           | connecting                                                            | The device is looking for a remote server.      |
|           | connected                                                             | The device is connected to the remote server.   |
|           | accepted                                                              | The device has accepted a new session.          |
|           | host-auth                                                             | host-to-host authentication is in progress.     |
|           | user-auth                                                             | User authentication is in progress.             |
|           | authenticated                                                         | User authentication is complete.                |
|           | open                                                                  | The session is in progress.                     |
|           | download                                                              | The user is downloading a file from the device. |
|           | upload                                                                | The user is uploading a file from the device.   |
|           | closing                                                               | The user is terminating the session.            |
|           | closed                                                                | The session is closed.                          |
| Filename  | Local filename of the file that the user is downloading or uploading. |                                                 |

**Related commands** [clear ssh](#)

# show ssh client

**Overview** This command displays the current configuration of the Secure Shell client.

**Syntax** `show ssh client`

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the current configuration for SSH clients on the login shell, use the command:

```
awplus# show ssh client
```

**Output** Figure 51-7: Example output from the **show ssh client** command

```
Secure Shell Client Configuration

Port : 22
Version : 2,1
Connect Timeout : 30 seconds
Session Timeout : 0 (off)
Debug : NONE
```

**Table 7:** Parameters in the output of the **show ssh client** command

| Parameter       | Description                                                                                                                                                 |
|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port            | SSH server TCP port where the SSH client connects to. The default is port 22.                                                                               |
| Version         | SSH server version, either "2" or "2,1". From AlliedWare Plus 5.5.1-1.1 onwards, SSH version 1 is not supported.                                            |
| Connect Timeout | Time in seconds that the SSH client waits for an SSH session to establish. If the value is 0, the connection is terminated when it reaches the TCP timeout. |
| Debug           | Whether debugging is active on the client.                                                                                                                  |

**Related commands** [show ssh server](#)

**Command changes** Version 5.5.3-1.1: added to AR1050V



# show ssh server

**Overview** This command displays the current configuration of the Secure Shell server.

Note that changes to the SSH configuration affects only new SSH sessions coming from remote hosts, and does not affect existing sessions.

**Syntax** `show ssh server`

**Mode** User Exec, Privileged Exec, and Global Configuration

**Example** To display the current configuration of the Secure Shell server, use the command:

```
awplus# show ssh server
```

**Output** Figure 51-8: Example output from the **show ssh server** command

```
Secure Shell Server Configuration

SSH Server : Enabled
Protocol : IPv4,IPv6
Port : 22
Version : 2
Services : scp, sftp
User Authentication : publickey, password
Resolve Hosts : Disabled
Session Timeout : 0 (Off)
Login Timeout : 60 seconds
Maximum Authentication Tries : 6
Maximum Startups : 10
Debug : NONE
Ciphers : aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr
KEX : curve25519-sha256@libssh.org,
 ecdh-sha2-nistp256,ecdh-sha2-nistp384,
 ecdh-sha2-nistp521,
 diffie-hellman-group-exchange-sha256,
 diffie-hellman-group-exchange-sha1,
 diffie-hellman-group14-sha1
```

**Table 8:** Parameters in the output of the **show ssh server** command

| Parameter  | Description                                                                                                      |
|------------|------------------------------------------------------------------------------------------------------------------|
| SSH Server | Whether the Secure Shell server is enabled or disabled.                                                          |
| Port       | TCP port where the Secure Shell server listens for connections. The default is port 22.                          |
| Version    | SSH server version; either '2' or '2,1'. From AlliedWare Plus 5.5.1-1.1 onwards, SSH version 1 is not supported. |
| Services   | List of the available Secure Shell services; one or more of SHELL, SCP or SFTP.                                  |

**Table 8:** Parameters in the output of the **show ssh server** command (cont.)

| Parameter           | Description                                                                                                                                                                          |
|---------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| User Authentication | List of available authentication methods.                                                                                                                                            |
| Login Timeout       | Time (in seconds) that the SSH server will wait the SSH session to establish. If the value is 0, the client login will be terminated when TCP timeout reaches.                       |
| Idle Timeout        | Time (in seconds) that the SSH server will wait to receive data from the SSH client. The server disconnects if this timer limit is reached. If set at 0, the idle timer remains off. |
| Maximum Startups    | The maximum number of concurrent connections that are waiting authentication. The default is 10.                                                                                     |
| Debug               | Whether debugging is active on the server.                                                                                                                                           |
| Ciphers             | List of ciphers permitted.                                                                                                                                                           |
| KEX                 | List of available Key Exchange algorithms.                                                                                                                                           |

**Related commands**   [show ssh](#)  
                              [show ssh client](#)

# show ssh server allow-users

**Overview** This command displays the user entries in the allow list of the SSH server.

**Syntax** `show ssh server allow-users`

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the user entries in the allow list of the SSH server, use the command:

```
awplus# show ssh server allow-users
```

**Output** Figure 51-9: Example output from the **show ssh server allow-users** command

| Username | Remote Hostname (pattern) |
|----------|---------------------------|
| awplus   | 192.168.*                 |
| john     |                           |
| manager  | *.alliedtelesis.com       |

**Table 9:** Parameters in the output of the **show ssh server allow-users** command

| Parameter                 | Description                                                                                                                                                                               |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username                  | User name that is allowed to access the SSH server.                                                                                                                                       |
| Remote Hostname (pattern) | IP address or hostname pattern of the remote client. The user is allowed requests from a host that matches this pattern. If no hostname is specified, the user is allowed from all hosts. |

**Related commands** [ssh server allow-users](#)  
[ssh server deny-users](#)

# show ssh server deny-users

**Overview** This command displays the user entries in the deny list of the SSH server. The user in the deny list is rejected to access the SSH server. If a user is not included in the access list of the SSH server, the user is also rejected.

**Syntax** `show ssh server deny-users`

**Mode** User Exec, Privileged Exec and Global Configuration

**Example** To display the user entries in the deny list of the SSH server, use the command:

```
awplus# show ssh server deny-users
```

**Output** Figure 51-10: Example output from the **show ssh server deny-users** command

| Username | Remote Hostname (pattern) |
|----------|---------------------------|
| john     | *.b-company.com           |
| manager  | 192.168.2.*               |

**Table 10:** Parameters in the output of the **show ssh server deny-user** command

| Parameter                 | Description                                                                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Username                  | The user that this rule applies to.                                                                                                                                                     |
| Remote Hostname (pattern) | IP address or hostname pattern of the remote client. The user is denied requests from a host that matches this pattern. If no hostname is specified, the user is denied from all hosts. |

**Related commands** [ssh server allow-users](#)  
[ssh server deny-users](#)

# ssh

**Overview** Use this command to initiate a Secure Shell connection to a remote SSH server.

If the server requests a password to login, you need to type in the correct password at the "Password:" prompt.

An SSH client identifies the remote SSH server by its public key registered on the client device. If the server identification is changed, server verification fails. If the public key of the server has been changed, the public key of the server must be explicitly added to the known host database.

**NOTE:** A hostname specified with SSH cannot begin with a hyphen (-) character.

**Syntax** `ssh [ip|ipv6] [user <username>|port <1-65535>|version 2]  
<remote-device> [<command>]`

| Parameter       | Description                                                                                                                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ip              | Specify IPv4 SSH.                                                                                                                                                                                                                                   |
| ipv6            | Specify IPv6 SSH.                                                                                                                                                                                                                                   |
| user            | Login user. If user is specified, the username is used for login to the remote SSH server when user authentication is required. Otherwise the current user name is used.<br><br><username> User name to login on the remote server.                 |
| port            | SSH server port. If port is specified, the SSH client connects to the remote SSH server with the specified TCP port. Otherwise, the client port configured by "ssh client" command or the default TCP port (22) is used.<br><br><1-65535> TCP port. |
| version         | SSH client version. From 5.5.1-1.1 onwards, SSH only supports version 2.                                                                                                                                                                            |
| <remote-device> | IPv4/IPv6 address or hostname of a remote server. The address is in the format A.B.C.D for an IPv4 address, or in the format X:X::X:X for an IPv6 address. Note that a hostname specified with SSH cannot begin with a hyphen (-) character.        |
| <command>       | A command to execute on the remote server. If a command is specified, the command is executed on the remote SSH server and the session is disconnected when the remote command finishes.                                                            |

**Mode** User Exec and Privileged Exec

**Examples** To login to the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 as user 'manager', use the command:

```
awplus# ssh ip user manager 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 that is listening on TCP port 2000, use the command:

```
awplus# ssh port 2000 192.0.2.5
```

To login to the remote SSH server 'example\_host' using an IPv6 session, use the command:

```
awplus# ssh ipv6 example_host
```

To run the **cmd** command on the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5 cmd
```

**Related  
commands**

[crypto key generate userkey](#)  
[crypto key pubkey-chain knownhosts](#)  
[debug ssh client](#)  
[ssh client](#)

**Command  
changes**

Version 5.5.3-1.1: added to AR1050V  
Version 5.5.1-1.1: support removed for SSH protocol v1  
Version 5.4.8-2.1: secure mode syntax added for x950, SBx908 GEN2.  
Version 5.4.8-1.2: secure mode syntax added for x220, x930, x550, XS900MX.  
Version 5.4.6-2.1: VRF-lite support added for AR-Series devices.

# ssh client

**Overview** This command modifies the default configuration parameters of the Secure Shell (SSH) client. The configuration is used for any SSH client on the device to connect to remote SSH servers. Any parameters specified on SSH client explicitly override the default configuration parameters.

The change affects the current user shell only. When the user exits the login session, the configuration does not persist. This command does not affect existing SSH sessions.

The **no** variant of this command resets configuration parameters of the Secure Shell (SSH) client changed by the [ssh client](#) command, and restores the defaults.

This command does not affect the existing SSH sessions.

**Syntax** `ssh client {port <1-65535>|version 2|session-timeout <0-3600>|connect-timeout <1-600>}`  
`no ssh client {port|version|session-timeout|connect-timeout}`

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                     |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| port            | The default TCP port of the remote SSH server. If an SSH client specifies an explicit port of the server, it overrides the default TCP port.<br>Default: 22                                                                                                                                                                                                     |
|                 | <1-65535> TCP port number.                                                                                                                                                                                                                                                                                                                                      |
| version         | The SSH version used by the client for SSH sessions.<br>From 5.5.1-1.1 onwards, the SSH client supports only version 2                                                                                                                                                                                                                                          |
| session-timeout | The global session timeout for SSH sessions. If the session timer lapses since the last time an SSH client received data from the remote server, the session is terminated. If the value is 0, then the client does not terminate the session. Instead, the connection is terminated when it reaches the TCP timeout.<br>Default: 0 (session timer remains off) |
|                 | <0-3600> Timeout in seconds.                                                                                                                                                                                                                                                                                                                                    |
| connect-timeout | The maximum time period that an SSH session can take to become established. The SSH client terminates the SSH session if this timeout expires and the session is still not established.<br>Default: 30                                                                                                                                                          |
|                 | <1-600> Timeout in seconds.                                                                                                                                                                                                                                                                                                                                     |

**Mode** Privileged Exec

**Examples** To configure the default TCP port for SSH clients to 2200, and the session timer to 10 minutes, use the command:

```
awplus# ssh client port 2200 session-timeout 600
```

To configure the connect timeout of SSH client to 10 seconds, use the command:

```
awplus# ssh client connect-timeout 10
```

To restore the connect timeout to its default, use the command:

```
awplus# no ssh client connect-timeout
```

**Related  
commands**    [show ssh client](#)  
              [ssh](#)

**Command  
changes**    Version 5.5.3-1.1: added to AR1050V  
              Version 5.5.2-1.1: **vrf** parameter added for products that support VRF  
              Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for  
              SSH protocol v1



# ssh client allow-legacy-ssh-rsa

**Overview** Use this command to enable support for the legacy ssh-rsa algorithm on the SSH client. Support for this algorithm was removed in version 5.5.1-1.1 due to security concerns. Support for it is still disabled by default and you should only enable it if you cannot avoid using ssh-rsa. It cannot be enabled when the device is in Secure Mode.

Use the **no** variant of this command to disable support for the legacy ssh-rsa algorithm on the SSH client.

**Syntax** `ssh client allow-legacy-ssh-rsa`  
`no ssh client allow-legacy-ssh-rsa`

**Default** Disabled

**Mode** Global Configuration

**Example** To enable SSH client support for the legacy ssh-rsa algorithm, use the commands:

```
awplus# configure terminal
awplus(config)# ssh client allow-legacy-ssh-rsa
```

**Related commands** [show ssh client](#)  
[ssh client](#)  
[ssh server allow-legacy-ssh-rsa](#)

**Command changes** Version 5.5.3-1.1: added to AR1050V  
Version 5.5.3-0.1: command added

# ssh server

**Overview** Use this command to modify the configuration of the SSH server. Changing these parameters affects new SSH sessions connecting to the device.

Use the **no** variant of this command to restore the configuration of a specified parameter to its default. The change affects the SSH server immediately if the server is running. Otherwise, the configuration is used when the server starts.

To enable the SSH server, use the [service ssh](#) command.

**Syntax** `ssh server <1-65535>`

`ssh server {[session-timeout <0-3600>] [login-timeout <1-600>]  
[max-startups <1-128>]}`

`no ssh server {[session-timeout] [login-timeout]  
[max-startups]}`

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-65535>       | The TCP port number that the server listens to for incoming SSH sessions.<br>Default: 22                                                                                                                                                                                                                                                                               |
| session-timeout | The maximum time period that the server waits before deciding that a session is inactive and should be terminated. The server considers the session inactive when it has not received any data from the client, and when the client does not respond to keep alive messages.<br>Default: 0 (session timer remains off).<br><br>Enter a timeout between 0-3600 seconds. |
| login-timeout   | The maximum time period the server waits before disconnecting an unauthenticated client.<br>Default: 60<br><br>Enter a timeout between 1- 600 seconds.                                                                                                                                                                                                                 |
| max-startups    | The maximum number of concurrent unauthenticated connections the server accepts. When the number of SSH connections awaiting authentication reaches the limit, the server drops any additional connections until authentication succeeds or the login timer expires for a connection.<br>Default: 10<br><br>Enter a number of sessions in the range of 1-128.          |

**Mode** Global Configuration

**Examples** To set the session timer of the SSH server to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server session-timeout 600
```

To set the login timeout of the SSH server to 30 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 30
```

To limit the number of SSH client connections waiting for authentication from the SSH server to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-startups 3
```

To return the limit on the number of waiting connections to the default of 10, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server max-startups
```

To support the SSH server with TCP port 2200, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server 2200
```

**Related commands**   [show ssh server](#)  
                          [ssh client](#)

**Command changes**   Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

# ssh server allow-legacy-ssh-rsa

**Overview** Use this command to enable support for the legacy ssh-rsa algorithm on the SSH server. Support for this algorithm was removed in version 5.5.1-1.1 due to security concerns. Support for it is still disabled by default and you should only enable it if you cannot avoid using ssh-rsa. It cannot be enabled when the device is in Secure Mode.

Use the **no** variant of this command to disable support for the legacy ssh-rsa algorithm on the SSH server.

**Syntax** `ssh server allow-legacy-ssh-rsa`  
`no ssh server allow-legacy-ssh-rsa`

**Default** Disabled

**Mode** Global Configuration

**Example** To enable SSH server support for the legacy ssh-rsa algorithm, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-legacy-ssh-rsa
```

**Related commands** [show ssh server](#)  
[ssh server](#)  
[ssh client allow-legacy-ssh-rsa](#)

**Command changes** Version 5.5.3-0.1: command added

# ssh server allow-users

**Overview** This command adds a username pattern to the allow list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is accepted.

When there are no registered users in the server's database of allowed users, the SSH server does not accept SSH sessions even when enabled.

SSH server also maintains the deny list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

The **no** variant of this command deletes a username pattern from the allow list of the SSH server. To delete an entry from the allow list, the username and hostname pattern should match exactly with the existing entry.

**Syntax** `ssh server allow-users <username-pattern> [<hostname-pattern>]`  
`no ssh server allow-users <username-pattern>`  
`[<hostname-pattern>]`

| Parameter                             | Description                                                                                                                                                                                                              |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;username-pattern&gt;</code> | The username pattern that users can match to. An asterisk acts as a wildcard character that matches any string of characters.                                                                                            |
| <code>&lt;hostname-pattern&gt;</code> | The host name pattern that hosts can match to. If specified, the server allows the user to connect only from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters. |

**Mode** Global Configuration

**Examples** To allow the user `john` to create an SSH session from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john
```

To allow the user `john` to create an SSH session from a range of IP address (from 192.168.1.1 to 192.168.1.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john 192.168.1.*
```

To allow the user `john` to create a SSH session from `a-company.com` domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john *.a-company.com
```

To delete the existing user entry `john 192.168.1.*` in the allow list, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no ssh server allow-users john 192.168.1.*
```

**Related  
commands**

[show running-config ssh](#)

[show ssh server allow-users](#)

[ssh server deny-users](#)

# ssh server authentication

**Overview** This command enables RSA public-key or password user authentication for SSH Server. Apply the **password** keyword with the **ssh server authentication** command to enable password authentication for users. Apply the **publickey** keyword with the **ssh server authentication** command to enable RSA public-key authentication for users.

Use the **no** variant of this command to disable RSA public-key or password user authentication for SSH Server. Apply the **password** keyword with the **no ssh authentication** command to disable password authentication for users. Apply the required **publickey** keyword with the **no ssh authentication** command to disable RSA public-key authentication for users.

**Syntax** `ssh server authentication {password|publickey}`  
`no ssh server authentication {password|publickey}`

| Parameter | Description                                             |
|-----------|---------------------------------------------------------|
| password  | Specifies user password authentication for SSH server.  |
| publickey | Specifies user publickey authentication for SSH server. |

**Default** Both RSA public-key authentication and password authentication are enabled by default.

**Mode** Global Configuration

**Usage** For password authentication to authenticate a user, password authentication for a user must be registered in the local user database or on an external RADIUS server, before using the **ssh server authentication password** command.

For RSA public-key authentication to authenticate a user, a public key must be added for the user, before using the **ssh server authentication publickey** command.

**Examples** To enable `password` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server authentication password
```

To enable `publickey` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server authentication publickey
```

To disable password authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server authentication password
```

To disable publickey authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server authentication publickey
```

**Related  
commands**

[crypto key pubkey-chain userkey](#)  
[service ssh](#)  
[show ssh server](#)



# ssh server deny-users

**Overview** This command adds a username pattern to the deny list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is rejected.

SSH server also maintains the allow list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

If a hostname pattern is specified, the user is denied from the hosts matching the pattern.

The **no** variant of this command deletes a username pattern from the deny list of the SSH server. To delete an entry from the deny list, the username and hostname pattern should match exactly with the existing entry.

**Syntax** `ssh server deny-users <username-pattern> [<hostname-pattern>]`  
`no ssh server deny-users <username-pattern>`  
`[<hostname-pattern>]`

| Parameter                             | Description                                                                                                                                                                                                                                                                 |
|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;username-pattern&gt;</code> | The username pattern that users can match to. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen, full stop and asterisk symbols. An asterisk acts as a wildcard character that matches any string of characters. |
| <code>&lt;hostname-pattern&gt;</code> | The host name pattern that hosts can match to. If specified, the server denies the user only when they connect from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters.                                             |

**Mode** Global Configuration

**Examples** To deny the user `john` to access SSH login from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john
```

To deny the user `john` to access SSH login from a range of IP address (from 192.168.2.1 to 192.168.2.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john 192.168.2.*
```

To deny the user `john` to access SSH login from `b-company.com` domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john*.b-company.com
```

To delete the existing user entry `john 192.168.2.*` in the deny list, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no ssh server deny-users john 192.168.2.*
```

**Related  
commands**

[show running-config ssh](#)

[show ssh server deny-users](#)

[ssh server allow-users](#)

# ssh server max-auth-tries

**Overview** Use this command to specify the maximum number of SSH authentication attempts that the device will allow.

Use the **no** variant of this command to return the maximum number of attempts to its default value of 6.

**Syntax** `ssh server max-auth-tries <1-32>`  
`no ssh server max-auth-tries`

| Parameter | Description                                                          |
|-----------|----------------------------------------------------------------------|
| <1-32>    | Maximum number of SSH authentication attempts the device will allow. |

**Default** 6 attempts

**Mode** Global Configuration

**Usage** By default, users must wait one second after a failed login attempt before trying again. You can increase this gap by using the command [aaa login fail-delay](#).

**Example** To set the maximum number of SSH authentication attempts to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-auth-tries 3
```

**Related commands** [show ssh server](#)

# ssh server resolve-host

**Overview** This command enables resolving an IP address from a host name using a DNS server for client host authentication.

The **no** variant of this command disables this feature.

**Syntax** `ssh server resolve-hosts`  
`no ssh server resolve-hosts`

**Default** This feature is disabled by default.

**Mode** Global Configuration

**Usage notes** Your device has a DNS Client that is enabled automatically when you add a DNS server to your device. Use the [ip name-server](#) command to add a DNS server to the list of servers that the device queries.

**Example** To resolve a host name using a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server resolve-hosts
```

**Related commands** [ip name-server](#)  
[show ssh server](#)  
[ssh server allow-users](#)  
[ssh server deny-users](#)

# ssh server scp

- Overview** This command enables the Secure Copy (SCP) service on the SSH server. Once enabled, the server accepts SCP requests from remote clients.
- You must enable the SSH server as well as this service before the device accepts SCP connections. The SCP service is enabled by default as soon as the SSH server is enabled.
- The **no** variant of this command disables the SCP service on the SSH server. Once disabled, SCP requests from remote clients are rejected.

**Syntax** `ssh server scp`  
`no ssh server scp`

**Mode** Global Configuration

**Examples** To enable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server scp
```

To disable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server scp
```

**Related commands** [show running-config ssh](#)  
[show ssh server](#)

# ssh server secure-algs

**Overview** Use this command to force the SSH server to only use ciphers, key exchange algorithms and Message Authentication Code (MAC) algorithms that are currently considered best-practice.

This command is the same as using all of the commands [ssh server secure-ciphers](#), [ssh server secure-hostkey](#), [ssh server secure-mac](#), and [ssh server secure-kex](#). However, it does not include the optional **exclude-nist-curves** parameter of [ssh server secure-kex](#).

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of algorithms.

**Syntax** `ssh server secure-algs`  
`no ssh server secure-algs`

**Default** Disabled.

**Mode** Global Configuration

**Usage notes** To see the list of algorithms, use the [show ssh server](#) command.

**Example** To force the SSH server to use best-practice algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-algs
```

**Related commands** [show ssh server](#)  
[ssh server](#)  
[ssh server secure-ciphers](#)  
[ssh server secure-hostkey](#)  
[ssh server secure-kex](#)  
[ssh server secure-mac](#)

**Command changes** Version 5.5.1-1.1: command added

# ssh server secure-ciphers

**Overview** Use this command to force the SSH server to only negotiate ciphers regarded as current best-practice.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of ciphers.

**Syntax** `ssh server secure-ciphers`  
`no ssh server secure-ciphers`

**Default** Not set

**Mode** Global Configuration

**Usage notes** To see the list of ciphers, use the [show ssh server](#) command.

**Example** To configure the SSH server to use best-practice ciphers, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-ciphers
```

**Related commands** [show ssh server](#)  
[ssh server](#)  
[ssh server secure-algs](#)  
[ssh server secure-hostkey](#)  
[ssh server secure-kex](#)  
[ssh server secure-mac](#)

**Command changes** Version 5.5.0-1.1: command added

# ssh server secure-hostkey

**Overview** Use this command to force the SSH server to only use hostkey algorithms that are currently considered best-practice. This excludes NIST curve-based hostkey algorithms.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of hostkey algorithms.

**Syntax** `ssh server secure-hostkey`  
`no ssh server secure-hostkey`

**Default** Disabled

**Mode** Global Configuration

**Usage notes** Using this command may reduce compatibility with older SSH clients.  
To see the list of hostkey algorithms, use the [show ssh server](#) command.

**Example** To force the SSH server to use best-practice hostkey algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-hostkey
```

**Related commands** [show ssh server](#)  
[ssh server](#)  
[ssh server secure-algs](#)  
[ssh server secure-ciphers](#)  
[ssh server secure-kex](#)  
[ssh server secure-mac](#)

**Command changes** Version 5.5.2-2.1: command added



# ssh server secure-kex

**Overview** Use this command to force the SSH server to only use key exchange algorithms that are currently considered best-practice.

For example, using this command stops the device from using the diffie-hellman-group-exchange-sha1 key exchange algorithm.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of key-exchange algorithms.

**Syntax** `ssh server secure-kex [exclude-nist-curves]`  
`no ssh server secure-kex`

| Parameter                        | Description                                                                                                          |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <code>exclude-nist-curves</code> | Also exclude all NIST key exchange algorithms. Using this parameter may reduce compatibility with older SSH clients. |

**Default** Disabled.

**Mode** Global Configuration

**Usage notes** To see the list of key exchange algorithms, use the [show ssh server](#) command.

**Example** To force the SSH server to use best-practice key-exchange algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-kex
```

**Related commands** [show ssh server](#)  
[ssh server](#)  
[ssh server secure-algs](#)  
[ssh server secure-ciphers](#)  
[ssh server secure-hostkey](#)  
[ssh server secure-mac](#)

**Command changes** Version 5.5.2-2.1: **exclude-nist-curves** parameter added  
Version 5.5.0-2.3: command added

# ssh server secure-mac

**Overview** Use this command to force the SSH server to only use Message Authentication Code (MAC) algorithms that are currently considered best-practice.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of MAC algorithms.

**Syntax** `ssh server secure-mac`  
`no ssh server secure-mac`

**Default** Disabled.

**Mode** Global Configuration

**Usage notes** To see the list of MAC algorithms, use the [show ssh server](#) command.

**Example** To force the SSH server to use best-practice MAC algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-mac
```

**Related commands** [show ssh server](#)  
[ssh server](#)  
[ssh server secure-algs](#)  
[ssh server secure-ciphers](#)  
[ssh server secure-hostkey](#)  
[ssh server secure-kex](#)

**Command changes** Version 5.5.1-1.1: command added

# ssh server sftp

- Overview** This command enables the Secure FTP (SFTP) service on the SSH server. Once enabled, the server accepts SFTP requests from remote clients.
- You must enable the SSH server as well as this service before the device accepts SFTP connections. The SFTP service is enabled by default as soon as the SSH server is enabled. If the SSH server is disabled, SFTP service is unavailable.
- The **no** variant of this command disables SFTP service on the SSH server. Once disabled, SFTP requests from remote clients are rejected.

**Syntax** `ssh server sftp`  
`no ssh server sftp`

**Mode** Global Configuration

**Examples** To enable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server sftp
```

To disable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server sftp
```

**Related commands** [show running-config ssh](#)  
[show ssh server](#)

# ssh server tcpforwarding

**Overview** Use this command to enable TCP port forwarding on the SSH server. It is disabled by default, to enhance security.

Use the **no** variant of this command to disable TCP port forwarding again.

**Syntax** `ssh server tcpforwarding`  
`no ssh server tcpforwarding`

**Default** Disabled

**Mode** Global Configuration

**Example** To enable TCP port forwarding, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server tcpforwarding
```

To disable it again, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server tcpforwarding
```

**Related commands** [show ssh server](#)

**Command changes** Version 5.5.2-1.1: command added

# undebug ssh client

**Overview** This command applies the functionality of the **no debug ssh client** command.

**Command changes** Version 5.5.3-1.1: added to AR1050V

# undebug ssh server

**Overview** This command applies the functionality of the **no debug ssh server** command.

# 52

# Trigger Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure Triggers. For more information, see the [Triggers Feature Overview and Configuration Guide](#).

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Command List**
- [“active \(trigger\)”](#) on page 2445
  - [“day”](#) on page 2446
  - [“debug trigger”](#) on page 2448
  - [“description \(trigger\)”](#) on page 2449
  - [“repeat”](#) on page 2450
  - [“script”](#) on page 2451
  - [“show debugging trigger”](#) on page 2453
  - [“show running-config trigger”](#) on page 2454
  - [“show trigger”](#) on page 2455
  - [“test”](#) on page 2460
  - [“time \(trigger\)”](#) on page 2461
  - [“trap”](#) on page 2463
  - [“trigger”](#) on page 2464
  - [“trigger activate”](#) on page 2465
  - [“type atmf guest”](#) on page 2466
  - [“type atmf node”](#) on page 2467
  - [“type cpu”](#) on page 2469
  - [“type interface”](#) on page 2470

- [“type linkmon-probe”](#) on page 2471
- [“type log”](#) on page 2473
- [“type memory”](#) on page 2474
- [“type periodic”](#) on page 2475
- [“type ping-poll”](#) on page 2476
- [“type reboot”](#) on page 2477
- [“type time”](#) on page 2478
- [“undebbug trigger”](#) on page 2479



# active (trigger)

**Overview** This command enables a trigger. This allows the trigger to activate when its trigger conditions are met.

The **no** variant of this command disables a trigger. While in this state the trigger cannot activate when its trigger conditions are met.

**Syntax** active  
no active

**Default** Active, which means that triggers are enabled by default

**Mode** Trigger Configuration

**Usage notes** Configure a trigger first before you use this command to activate it.

For information about configuring a trigger, see the [Triggers\\_Feature Overview and Configuration Guide](#).

**Examples** To enable trigger 172, so that it can activate when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 172
awplus(config-trigger)# active
```

To disable trigger 182, preventing it from activating when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 182
awplus(config-trigger)# no active
```

**Related commands** [show trigger](#)  
[trigger](#)  
[trigger activate](#)

# day

**Overview** This command specifies the days or date that the trigger can activate on. You can specify one of:

- A specific date
- A specific day of the week
- A list of days of the week
- A day of any month of any year
- A day of a specific month in any year
- Every day

By default, the trigger can activate on any day.

**Syntax** `day every-day`  
`day <1-31>`  
`day <1-31> <month>`  
`day <1-31> <month> <year>`  
`day <weekday>`

| Parameter                    | Description                                                                                                                                                                                                                 |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>every-day</code>       | Sets the trigger so that it can activate on any day.                                                                                                                                                                        |
| <code>&lt;1-31&gt;</code>    | Day of the month the trigger is permitted to activate on.                                                                                                                                                                   |
| <code>&lt;month&gt;</code>   | Sets the month that the trigger is permitted to activate on. Valid keywords are: <b>january, february, march, april, may, june, july, august, september, october, november, and december.</b>                               |
| <code>&lt;year&gt;</code>    | Sets the year that the trigger is permitted to activate in, between 2000 and 2035.                                                                                                                                          |
| <code>&lt;weekday&gt;</code> | Sets the days of the week that the trigger can activate on. You can specify one or more week days in a space separated list. Valid keywords are: <b>monday, tuesday, wednesday, thursday, friday, saturday, and sunday.</b> |

**Default** **every-day**, so by default, the trigger can activate on any day.

**Mode** Trigger Configuration

**Usage notes** For example trigger configurations that use the **day** command, see “Restrict Internet Access” and “Turn off Power to Port LEDs” in the [Triggers Feature Overview and Configuration Guide](#).

**Examples** To permit trigger 55 to activate on the 1 June 2019, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 55
awplus(config-trigger)# day 1 jun 2019
```

To permit trigger 12 to activate on Mondays, Wednesdays and Fridays, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# day monday wednesday friday
```

To permit trigger 17 to activate on the 5th day of any month, in any year, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 17
awplus(config-trigger)# day 5
```

To permit trigger 6 to activate on the 20th day of September, in any year, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 6
awplus(config-trigger)# day 20 september
```

To permit trigger 14 to activate on the 1st day of each month, in any year, at 11.00am, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 14
awplus(config-trigger)# day 1
awplus(config-trigger)# type time 11:00
```

**Related commands** [show trigger](#)  
[type time](#)  
[trigger](#)

**Command changes** Version 5.4.8-2.1: day of the month functionality added

# debug trigger

**Overview** This command enables trigger debugging. This generates detailed messages about how your device is processing the trigger commands and activating the triggers.

The **no** variant of this command disables trigger debugging.

**Syntax** `debug trigger`  
`no debug trigger`

**Mode** Privilege Exec

**Examples** To start trigger debugging, use the command:

```
awplus# debug trigger
```

To stop trigger debugging, use the command:

```
awplus# no trigger
```

**Related commands** [show debugging trigger](#)  
[show trigger](#)  
[test](#)  
[trigger](#)  
[undebug trigger](#)

# description (trigger)

**Overview** This command adds an optional description to help you identify the trigger. This description is displayed in show command outputs and log messages.

The **no** variant of this command removes a trigger's description. The show command outputs and log messages stop displaying a description for this trigger.

**Syntax** `description <description>`  
`no description`

| Parameter                        | Description                                                                                                                                                       |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;description&gt;</code> | A word or phrase that uniquely identifies this trigger or its purpose. Valid characters are any printable character and spaces, up to a maximum of 40 characters. |

**Mode** Trigger Configuration

**Examples** To give trigger 240 the description `daily status report`, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 240
awplus(config-trigger)# description daily status report
```

To remove the description from trigger 36, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 36
awplus(config-trigger)# no description
```

**Related commands** [show trigger](#)  
[test](#)  
[trigger](#)

# repeat

**Overview** This command specifies the number of times that a trigger is permitted to activate. This allows you to specify whether you want the trigger to activate:

- only the first time that the trigger conditions are met
- a limited number of times that the trigger conditions are met
- an unlimited number of times

Once the trigger has reached the limit set with this command, the trigger remains in your configuration but cannot be activated. Use the **repeat** command again to reset the trigger so that it is activated when its trigger conditions are met.

By default, triggers can activate an unlimited number of times. To reset a trigger to this default, specify either **yes** or **forever**.

**Syntax** `repeat {forever|no|once|yes|<1-4294967294>}`

| Parameter                         | Description                                          |
|-----------------------------------|------------------------------------------------------|
| <code>yes forever</code>          | The trigger repeats indefinitely, or until disabled. |
| <code>no once</code>              | The trigger activates only once.                     |
| <code>&lt;1-4292967294&gt;</code> | The trigger repeats the specified number of times.   |

**Mode** Trigger Configuration

**Examples** To allow trigger 21 to activate only once, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 21
awplus(config-trigger)# repeat no
```

To allow trigger 22 to activate an unlimited number of times whenever its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 22
awplus(config-trigger)# repeat forever
```

To allow trigger 23 to activate only the first 10 times the conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 23
awplus(config-trigger)# repeat 10
```

**Related commands** [show trigger](#)  
[trigger](#)

# script

**Overview** This command specifies one or more scripts that are to be run when the trigger activates. You can add up to five scripts to a single trigger.

The sequence in which the trigger runs the scripts is specified by the number you set before the name of the script file. One script is executed completely before the next script begins.

Scripts may be either ASH shell scripts, indicated by a **.sh** filename extension suffix, or AlliedWare Plus scripts, indicated by a **.scp** filename extension suffix. AlliedWare Plus scripts only need to be readable.

The **no** variant of this command removes one or more scripts from the trigger's script list. The scripts are identified by either their name, or by specifying their position in the script list. The **all** parameter removes all scripts from the trigger.

**Syntax** `script <1-5> {<filename>}`  
`no script {<1-5>|<filename>|all}`

| Parameter  | Description                                                                                          |
|------------|------------------------------------------------------------------------------------------------------|
| <1-5>      | The position of the script in execution sequence. The trigger runs the lowest numbered script first. |
| <filename> | The path to the script file.                                                                         |

**Mode** Trigger Configuration

**Examples** To configure trigger 71 to run the script flash:/cpu\_trig.sh in position 3 when the trigger activates, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# script 3 flash:/cpu_trig.sh
```

To configure trigger 99 to run the scripts flash:reconfig.scp, flash:cpu\_trig.sh and flash:email.scp in positions 2, 3 and 5 when the trigger activates, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 99
awplus(config-trigger)# script 2 flash:/reconfig.scp 3
flash:/cpu_trig.sh 5 flash:/email.scp
```

To remove the scripts 1, 3 and 4 from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script 1 3 4
```

To remove the script flash:/cpu\_trig.sh from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script flash:/cpu_trig.sh
```

To remove all the scripts from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script all
```

**Related  
commands**   [show trigger](#)  
[trigger](#)



# show debugging trigger

**Overview** This command displays the current status for trigger utility debugging. Use this command to show when trigger debugging has been turned on or off from the [debug trigger](#) command.

**Syntax** show debugging trigger

**Mode** User Exec and Privileged Exec

**Example** To display the current configuration of trigger debugging, use the command:  
awplus# show debugging trigger

**Output** Figure 52-1: Example output from the **show debugging trigger** command

```
awplus#debug trigger
awplus#show debugging trigger
Trigger debugging status:
 Trigger debugging is on

awplus#no debug trigger
awplus#show debugging trigger
Trigger debugging status:
 Trigger debugging is off
```

**Related commands** [debug trigger](#)

# show running-config trigger

**Overview** This command displays the current running configuration of the trigger utility.

**Syntax** `show running-config trigger`

**Mode** Privileged Exec

**Example** To display the current configuration of the trigger utility, use the command:

```
awplus# show running-config trigger
```

Figure 52-2: Example output from the **show running-config trigger** command

```
trigger 1
 type card in

type usb in
 trigger 2

type usb out
 !
```

**Related commands** [show trigger](#)

# show trigger

**Overview** This command displays configuration and diagnostic information about the triggers configured on the device. Specify the **show trigger** command without any options to display a summary of the configuration of all triggers.

**Syntax** `show trigger [<1-250>|counter|full]`

| Parameter | Description                                                                           |
|-----------|---------------------------------------------------------------------------------------|
| <1-250>   | Displays detailed information about a specific trigger, identified by its trigger ID. |
| counter   | Displays statistical information about all triggers.                                  |
| full      | Displays detailed information about all triggers.                                     |

**Mode** Privileged Exec

**Example** To get summary information about all triggers, use the following command:

```
awplus# show trigger
```

Table 52-1: Example output from **show trigger**

| awplus#show trigger |                   |                      |    |    |            |      |           |
|---------------------|-------------------|----------------------|----|----|------------|------|-----------|
| TR#                 | Type & Details    | Name                 | Ac | Te | Repeat     | #Scr | Days/Date |
| 001                 | CPU (80% any)     | Busy CPU             | Y  | N  | 5          | 1    | smtwtfs   |
| 005                 | Periodic (30 min) | Regular status check | Y  | N  | Continuous | 1    | -mtwtf-   |
| 007                 | Memory (85% up)   | High mem usage       | Y  | N  | 8          | 1    | smtwtfs   |
| 011                 | Time (00:01)      | Weekend access       | Y  | N  | Continuous | 1    | -----s    |
| 013                 | Reboot            |                      | Y  | N  | Continuous | 2    | smtwtfs   |
| 019                 | Ping-poll (5 up)  | Connection to svrl   | Y  | N  | Continuous | 1    | smtwtfs   |

Table 52-2: Parameters in the output of **show trigger**

| Parameter      | Description                                                                                        |
|----------------|----------------------------------------------------------------------------------------------------|
| TR#            | Trigger identifier (ID).                                                                           |
| Type & Details | The trigger type, followed by the trigger details in brackets.                                     |
| Name           | Descriptive name of the trigger configured with the <a href="#">description (trigger)</a> command. |
| Ac             | Whether the trigger is active (Y), or inactive (N).                                                |
| Te             | Whether the trigger is in test mode (Y) or not (N).                                                |

Table 52-2: Parameters in the output of **show trigger** (cont.)

| Parameter | Description                                                                                                                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Repeat    | Whether the trigger repeats continuously, and if not, the configured repeat count for the trigger. To see the number of times a trigger has activated, use the <b>show trigger</b> <1-250> command.                 |
| #Scr      | Number of scripts associated with the trigger.                                                                                                                                                                      |
| Days/Date | Days or date when the trigger may be activated. For the days options, the days are shown as a seven character string representing Sunday to Saturday. A hyphen indicates days when the trigger cannot be activated. |

To display detailed information about trigger 3, use the command:

```
awplus# show trigger 3
```

Figure 52-3: Example output from **show trigger** for a specific trigger

```
awplus#show trigger 1
Trigger Configuration Details

Trigger 1
Name display cpu usage when pass 80%
Type and details CPU (80% up)
Days smtwtfS
Active Yes
Test No
Trap Yes
Repeat Continuous
Modified Fri Feb 3 17:18:44 2017
Number of activations 0
Last activation not activated
Number of scripts 1
1. shocpu.scp
2.
3.
4.
5.

```

To display detailed information about all triggers, use the command:

```
awplus# show trigger full
```

Table 52-3: Example output from **show trigger full**

```

awplus#show trigger full
Trigger Configuration Details

Trigger 1
Name Busy CPU
Type and details CPU (80% up)
Days smtwtfss
Active Yes
Test No
Trap Yes
Repeat Continuous
Modified Fri Feb 3 17:05:16 2017
Number of activations 0
Last activation not activated
Number of scripts 2
 1. flash:/cpu_alert.sh
 2. flash:/reconfig.scp
 3.
 4.
 5.
Trigger 5
Name Regular status check
Type and details Periodic (30 min)
Days smtwtfss
Active Yes
Test No
Trap Yes
Repeat 5 (2)
Modified Fri Feb 3 17:18:44 2017
Number of activations 0
Last activation Fri Feb 10 18:00:00 2017
Number of scripts 1
 1. flash:/stat_check.scp
 2.
 3.
 4.
 5.

```

**Table 53:** Parameters in the output of **show trigger full** and **show trigger** for a specific trigger

| Parameter        | Description                                             |
|------------------|---------------------------------------------------------|
| Trigger          | The ID of the trigger.                                  |
| Name             | Descriptive name of the trigger.                        |
| Type and details | The trigger type and its activation conditions.         |
| Days             | The days on which the trigger is permitted to activate. |

**Table 53:** Parameters in the output of **show trigger full** and **show trigger** for a specific trigger (cont.)

| Parameter             | Description                                                                                                                                                                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Date                  | The date on which the trigger is permitted to activate. Only displayed if configured, in which case it replaces "Days".                                                                                                                       |
| Active                | Whether or not the trigger is permitted to activate.                                                                                                                                                                                          |
| Test                  | Whether or not the trigger is operating in diagnostic mode.                                                                                                                                                                                   |
| Trap                  | Whether or not the trigger is enabled to send SNMP traps.                                                                                                                                                                                     |
| Repeat                | Whether the trigger repeats an unlimited number of times (Continuous) or for a set number of times. When the trigger can repeat only a set number of times, then the number of times the trigger has been activated is displayed in brackets. |
| Modified              | The date and time of the last time that the trigger was modified.                                                                                                                                                                             |
| Number of activations | Number of times the trigger has been activated since the last restart of the device.                                                                                                                                                          |
| Last activation       | The date and time of the last time that the trigger was activated.                                                                                                                                                                            |
| Number of scripts     | How many scripts are associated with the trigger, followed by the names of the script files in the order in which they run.                                                                                                                   |

To display counter information about all triggers use the command:

```
awplus# show trigger counter
```

**Figure 52-4:** Example output from **show trigger counter**

```
awplus# show trigger counter
Trigger Module Counters

Trigger activations 4
Last trigger activated 55
Time triggers activated today 0
Periodic triggers activated today 0
Interface triggers activated today 1
CPU triggers activated today 2
Memory triggers activated today 1
Reboot triggers activated today 0
Ping-poll triggers activated today 0
USB event triggers activated today 0
Stack master fail triggers activated today 0
Stack member triggers activated today 0
Stack link triggers activated today 0
ATMF node triggers activated today 0
ATMF guest triggers activated today 0
Log triggers activated today 0

```

**Related  
commands**

- [active \(trigger\)](#)
- [debug trigger](#)
- [script](#)
- [trigger](#)
- [trigger activate](#)

# test

**Overview** This command puts the trigger into a diagnostic mode. In this mode the trigger may activate but when it does it will not run any of the trigger's scripts. A log message will be generated to indicate when the trigger has been activated.

The **no** variant of this command takes the trigger out of diagnostic mode, restoring normal operation. When the trigger activates, the scripts associated with the trigger will be run, as normal.

**Syntax** test  
no test

**Mode** Trigger Configuration

**Usage notes** Configure a trigger first before you use this command to diagnose it. For information about configuring a trigger, see the [Triggers\\_Feature Overview and Configuration Guide](#).

**Examples** To put trigger 5 into diagnostic mode, where no scripts will be run when the trigger activates, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# test
```

To take trigger 205 out of diagnostic mode, restoring normal operation, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no test
```

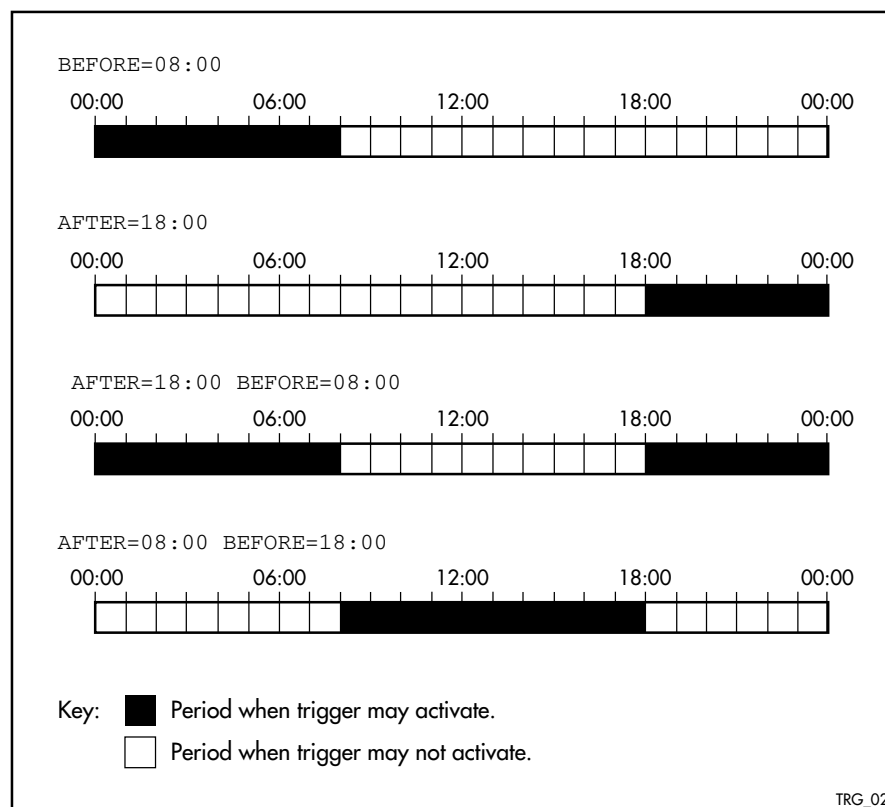
**Related commands** [show trigger](#)  
[trigger](#)



# time (trigger)

**Overview** This command specifies the time of day when the trigger is permitted to activate. The **after** parameter specifies the start of a time period that extends to midnight during which trigger may activate. By default the value of this parameter is 00:00:00 (am); that is, the trigger may activate at any time. The **before** parameter specifies the end of a time period beginning at midnight during which the trigger may activate. By default the value of this parameter is 23:59:59; that is, the trigger may activate at any time. If the value specified for **before** is later than the value specified for **after**, a time period from “after” to “before” is defined, during which the trigger may activate. This command is not applicable to time triggers ( **type time** ).

The following figure illustrates how the **before** and **after** parameters operate.



**Syntax** `time {[after <hh:mm:ss>] [before <hh:mm:ss>]}`

| Parameter        | Description                                                 |
|------------------|-------------------------------------------------------------|
| after<hh:mm:ss>  | The earliest time of day when the trigger may be activated. |
| before<hh:mm:ss> | The latest time of day when the trigger may be activated.   |

**Mode** Trigger Configuration

**Usage notes** For example trigger configurations that use the **time (trigger)** command, see “Restrict Internet Access” and “Turn off Power to Port LEDs” in the [Triggers Feature Overview and Configuration Guide](#).

**Examples** To allow trigger 63 to activate between midnight and 10:30am, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 63
awplus(config-trigger)# time before 10:30:00
```

To allow trigger 64 to activate between 3:45pm and midnight, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 64
awplus(config-trigger)# time after 15:45:00
```

To allow trigger 65 to activate between 10:30am and 8:15pm, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 65
awplus(config-trigger)# time after 10:30:00 before 20:15:00
```

**Related commands** [show trigger](#)  
[trigger](#)

# trap

**Overview** This command enables the specified trigger to send SNMP traps.  
Use the **no** variant of this command to disable the sending of SNMP traps from the specified trigger.

**Syntax** trap  
no trap

**Default** SNMP traps are enabled by default for all defined triggers.

**Mode** Trigger Configuration

**Usage notes** You must configure SNMP before using traps with triggers. For more information, see:

- [Support for Allied Telesis Enterprise\\_MIBs\\_in\\_AlliedWare Plus](#), for information about which MIB objects are supported.
- the [SNMP Feature Overview and Configuration\\_Guide](#).
- the [SNMP Commands](#) chapter.

Since SNMP traps are enabled by default for all defined triggers, a common usage will be for the **no** variant of this command to disable SNMP traps from a specified trap if the trap is only periodic. Refer in particular to AT-TRIGGER-MIB in the [Support for Allied Telesis Enterprise\\_MIBs\\_in AlliedWare Plus](#) for further information about the relevant SNMP MIB.

**Examples** To enable SNMP traps to be sent from trigger 5, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# trap
```

To disable SNMP traps being sent from trigger 205, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no trap
```

**Related commands** trigger  
show trigger

# trigger

**Overview** This command is used to access the Trigger Configuration mode for the specified trigger. Once Trigger Configuration mode has been entered the trigger type information can be configured and the trigger scripts and other operational parameters can be specified. At a minimum the trigger type information must be specified before the trigger can become active.

The **no** variant of this command removes a specified trigger and all configuration associated with it.

**Syntax** trigger <1-250>  
no trigger <1-250>

| Parameter | Description   |
|-----------|---------------|
| <1-250>   | A trigger ID. |

**Mode** Global Configuration

**Examples** To enter trigger configuration mode for trigger 12, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 12
```

To completely remove all configuration associated with trigger 12, use the commands:

```
awplus# configure terminal
awplus(config)# no trigger 12
```

**Related commands** [show trigger](#)  
[trigger activate](#)

# trigger activate

**Overview** This command is used to manually activate a specified trigger from the Privileged Exec mode, which has been configured with the **trigger** command from the Global Configuration mode.

**Syntax** `trigger activate <1-250>`

| Parameter | Description   |
|-----------|---------------|
| <1-250>   | A trigger ID. |

**Mode** Privileged Exec

**Usage notes** This command manually activates a trigger without the normal trigger conditions being met.

The trigger is activated even if it has been configured as inactive by using the command **no active**. The scripts associated with the trigger will be executed even if the trigger is in the diagnostic test mode.

Triggers activated manually do not have their repeat counts decremented or their 'last triggered' time updated, and do not result in updates to the '[type] triggers today' counters.

**Example** To manually activate trigger 12 use the command:

```
awplus# trigger activate 12
```

**Related commands** [active \(trigger\)](#)  
[show trigger](#)  
[trigger](#)

# type atmf guest

**Overview** This command configures a trigger to activate when an AMF guest node joins or leaves.

**Syntax** `type atmf guest {join|leave}`

| Parameter | Description            |
|-----------|------------------------|
| join      | AMF guest node joins.  |
| leave     | AMF guest node leaves. |

**Mode** Trigger Configuration

**Example** To configure trigger 86 to activate when an AMF guest node leaves, use the following commands:

```
awplus(config)# trigger 86
awplus(config-trigger)# type atmf guest leave
```

**Related commands** [show trigger](#)

**Command changes** Version 5.5.1-1.1: command added

# type atmf node

**Overview** This command configures a trigger to activate when an AMF node joins or leaves.

**Syntax** type atmf node {join|leave}

| Parameter | Description      |
|-----------|------------------|
| join      | AMF node joins.  |
| leave     | AMF node leaves. |

**Mode** Trigger Configuration

**Example 1** To configure trigger 5 to activate when an AMF node leaves, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger)# type atmf node leave
```

**Example 2** The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
=====
node1, node2, node3:
=====

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

## Display the trigger configurations

AMF-Net[3]# show trigger

This command returns the following display:

```
=====
node1:
=====
```

| TR# | Type & Details    | Description         | Ac | Te | Tr | Repeat     | #Scr | Days/Date |
|-----|-------------------|---------------------|----|----|----|------------|------|-----------|
| 001 | Periodic (2 min)  | Periodic Status Chk | Y  | N  | Y  | Continuous | 1    | smtwtfs   |
| 005 | ATMF node (leave) | E-mail on ATMF Exit | Y  | N  | Y  | Continuous | 1    | smtwtfs   |

```

=====
Node2, Node3,
=====
```

| TR# | Type & Details    | Description         | Ac | Te | Tr | Repeat     | #Scr | Days/Date |
|-----|-------------------|---------------------|----|----|----|------------|------|-----------|
| 005 | ATMF node (leave) | E-mail on ATMF Exit | Y  | N  | Y  | Continuous | 1    | smtwtfs   |

```

```

## Display the triggers configured on each of the nodes in the AMF Network.

AMF-Net[3]# show running-config trigger

This command returns the following display:

```
=====
Node1:
=====

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!

=====
Node2, Node3:
=====

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

**Related commands** [show trigger](#)



# type cpu

**Overview** This command configures a trigger to activate based on CPU usage level. Selecting the **up** option causes the trigger to activate when the CPU usage exceeds the specified usage level. Selecting the **down** option causes the trigger to activate when CPU usage drops below the specified usage level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

**Syntax** `type cpu <1-100> [up|down|any]`

| Parameter | Description                                                            |
|-----------|------------------------------------------------------------------------|
| <1-100>   | The percentage of CPU usage at which to trigger.                       |
| up        | Activate when CPU usage exceeds the specified level.                   |
| down      | Activate when CPU usage drops below the specified level                |
| any       | Activate when CPU usage passes the specified level in either direction |

**Mode** Trigger Configuration

**Usage notes** For an example trigger configuration that uses the **type cpu** command, see “Capture Unusual CPU and RAM Activity” in the [Triggers Feature Overview and Configuration Guide](#).

**Examples** To configure trigger 28 to be a CPU trigger that activates when CPU usage exceeds 80% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 28
awplus(config-trigger)# type cpu 80 up
```

To configure trigger 5 to be a CPU trigger that activates when CPU usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65

or

awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65 any
```

**Related commands** [show trigger](#)  
[trigger](#)

# type interface

**Overview** This command configures a trigger to activate based on the link status of an interface. The trigger can be activated when the interface becomes operational by using the **up** option, or when the interface closes by using the **down** option. The trigger can also be configured to activate when either one of these events occurs by using the **any** option.

**Syntax** `type interface <interface> {up|down|any}`

| Parameter   | Description                                           |
|-------------|-------------------------------------------------------|
| <interface> | Interface name.                                       |
| up          | Activate when interface becomes operational.          |
| down        | Activate when the interface closes.                   |
| any         | Activate when any interface link status event occurs. |

**Mode** Trigger Configuration

**Example** To configure trigger 19 to be an interface trigger that activates when eth0 becomes operational, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 19
awplus(config-trigger)# type interface eth0 up
```

**Related commands** [show trigger](#)  
[trigger](#)

# type linkmon-probe

**Overview** Use this command to create a trigger that will run a script when a Link Health Monitoring probe reports that a link becomes “good”, “bad”, or “unreachable”.

**Syntax** `type linkmon-probe <probename> <profilename>  
{good|bad|unreachable|any}`

| Parameter     | Description                                                                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <probename>   | The name of the Link Health Monitoring probe that will be used for executing the trigger.                                                                    |
| <profilename> | The name of the Link Health Monitoring performance profile that will be used for determine if the Link Health Monitoring probe is good, bad, or unreachable. |
| good          | If the Link Health Monitoring probe becomes 'good' according to the Link Health Monitoring performance profile then the trigger will be executed.            |
| bad           | If the Link Health Monitoring probe goes 'bad' according to the Link Health Monitoring performance profile then the trigger will be executed.                |
| unreachable   | If the Link Health Monitoring probe becomes 'unreachable' according to the Link Health Monitoring performance profile then the trigger will be executed.     |
| any           | If the Link Health Monitoring probe changes state according to the Link Health Monitoring performance profile then the trigger will be executed.             |

**Mode** Trigger Configuration

**Example** When the Link Health Monitoring probes sent to the “test-probe” destination no longer meet the performance profile “test-profile” the link will be deemed “bad”. To create a trigger that will run a script when a Link Health Monitoring probe is deemed “bad”, use the following commands:

```
awplus(config)# trigger 1
awplus(config-trigger)# script 1 link-bad.scp
awplus(config-trigger)# type linkmon-probe test-probe
test-profile bad
```

To create a trigger that will run a script when the link is deemed “good” again, use the following commands:

```
awplus(config)# trigger 2
awplus(config-trigger)# script 1 link-good.scp
awplus(config-trigger)# type linkmon-probe test-probe
test-profile good
```

**Related commands** [trigger](#)

**Command changes** Version 5.4.8-1.1: command added

# type log

**Overview** Use this command to configure a trigger to activate based on the content of log messages matching a string or regular expression.

**Syntax** `type log <log-message-string>`

| Parameter                               | Description                                                                              |
|-----------------------------------------|------------------------------------------------------------------------------------------|
| <code>&lt;log-message-string&gt;</code> | A string or a regular expression (PCRE) to match a log message or part of a log message. |

**Default** There is no type or log message string set by default.

**Mode** Trigger Configuration

**Usage notes** Log type triggers fully support regular expressions using PCRE (Perl-Compatible Regular Expression) syntax.

Only log messages of severity level notice or higher can activate a trigger.

Note that any command executed by the script will generate a log message with level notice, and will include '[SCRIPT]' before the command string. Therefore, if something in the script matches the configured log message trigger string, it will retrigger indefinitely.

**Example** To configure trigger 6 to activate when a log message of level notice or higher indicates that any port has 'failed', use the commands:

```
awplus# configure terminal
awplus(config)# trigger 6
awplus(config-trigger)# type log port.+ failed
```

**Related commands** [show trigger](#)  
[trigger](#)

**Command changes** Version 5.4.7-2.1: command added

# type memory

**Overview** This command configures a trigger to activate based on RAM usage level. Selecting the **up** option causes the trigger to activate when memory usage exceeds the specified level. Selecting the **down** option causes the trigger to activate when memory usage drops below the specified level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

**Syntax** `type memory <1-100> [up|down|any]`

| Parameter | Description                                                                |
|-----------|----------------------------------------------------------------------------|
| <1-100>   | The percentage of memory usage at which to trigger.                        |
| up        | Activate when memory usage exceeds the specified level.                    |
| down      | Activate when memory usage drops below the specified level.                |
| any       | Activate when memory usage passes the specified level in either direction. |

**Mode** Trigger Configuration

**Examples** To configure trigger 12 to be a memory trigger that activates when memory usage exceeds 50% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# type memory 50 up
```

To configure trigger 40 to be a memory trigger that activates when memory usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65
```

or

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65 any
```

**Related commands** [show trigger](#)  
[trigger](#)

# type periodic

**Overview** This command configures a trigger to be activated at regular intervals. The time period between activations is specified in minutes.

**Syntax** type periodic <1-1440>

| Parameter | Description                                |
|-----------|--------------------------------------------|
| <1-1440>  | The number of minutes between activations. |

**Mode** Trigger Configuration

**Usage notes** A combined limit of 10 triggers of the type periodic and time can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or
periodic
```

For an example trigger configuration that uses the **type periodic** command, see “See Daily Statistics” in the [Triggers\\_Feature Overview and Configuration Guide](#).

**Example** To configure trigger 44 to activate periodically at 10 minute intervals use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 44
awplus(config-trigger)# type periodic 10
```

**Related commands** [show trigger](#)  
[trigger](#)

# type ping-poll

**Overview** This command configures a trigger that activates when Ping Polling identifies that a target device's status has changed. This allows you to run a configuration script when a device becomes reachable or unreachable.

**Syntax** `type ping-poll <1-100> {up|down}`

| Parameter | Description                                                                     |
|-----------|---------------------------------------------------------------------------------|
| <1-100>   | The ping poll ID.                                                               |
| up        | The trigger activates when ping polling detects that the target is reachable.   |
| down      | The trigger activates when ping polling detects that the target is unreachable. |

**Mode** Trigger Configuration

**Example** To configure trigger 106 to activate when ping poll 12 detects that its target device is now unreachable, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 106
awplus(config-trigger)# type ping-poll 12 down
```

**Related commands** [show trigger](#)  
[trigger](#)



# type reboot

**Overview** This command configures a trigger that activates when your device is rebooted.

**Syntax** `type reboot`

**Mode** Trigger Configuration

**Example** To configure trigger 32 to activate when your device reboots, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 32
awplus(config-trigger)# type reboot
```

**Related commands** [show trigger](#)  
[trigger](#)

# type time

**Overview** This command configures a trigger that activates at a specified time of day.

**Syntax** `type time <hh:mm>`

| Parameter                  | Description                       |
|----------------------------|-----------------------------------|
| <code>&lt;hh:mm&gt;</code> | The time to activate the trigger. |

**Mode** Trigger Configuration

**Usage** A combined limit of 10 triggers of the type time and type periodic can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or
periodic
```

**Example** To configure trigger 86 to activate at 15:53, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type time 15:53
```

**Related commands** [show trigger](#)  
[trigger](#)

# undebbug trigger

**Overview** This command applies the functionality of the **no debug trigger** command.

# 53

# Ping-Polling Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure Ping Polling. For more information, see the [Ping Polling Feature Overview and Configuration Guide](#).

For information on filtering and saving command output, see the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Table 53-1: The following table lists the default values when configuring a ping poll

| Default           | Value                                                                       |
|-------------------|-----------------------------------------------------------------------------|
| Critical-interval | 1 second                                                                    |
| Description       | No description                                                              |
| Fail-count        | 5                                                                           |
| Length            | 32 bytes                                                                    |
| Normal-interval   | 30 seconds                                                                  |
| Sample-size       | 5                                                                           |
| Source-ip         | The IP address of the interface from which the ping packets are transmitted |
| Time-out          | 1 second                                                                    |
| Up-count          | 30                                                                          |

- Command List**
- [“active \(ping-polling\)”](#) on page 2482
  - [“clear ping-poll”](#) on page 2483
  - [“critical-interval”](#) on page 2484
  - [“debug ping-poll”](#) on page 2485

- [“description \(ping-polling\)”](#) on page 2486
- [“fail-count”](#) on page 2487
- [“ip \(ping-polling\)”](#) on page 2488
- [“length \(ping-poll data\)”](#) on page 2489
- [“normal-interval”](#) on page 2490
- [“ping-poll”](#) on page 2491
- [“sample-size”](#) on page 2492
- [“show counter ping-poll”](#) on page 2494
- [“show ping-poll”](#) on page 2496
- [“source-ip”](#) on page 2500
- [“timeout \(ping polling\)”](#) on page 2502
- [“up-count”](#) on page 2503
- [“undebg ping-poll”](#) on page 2504

# active (ping-polling)

**Overview** This command enables a ping-poll instance. The polling instance sends ICMP echo requests to the device with the IP address specified by the [ip \(ping-polling\)](#) command.

By default, polling instances are disabled. When a polling instance is enabled, it assumes that the device it is polling is unreachable.

The **no** variant of this command disables a ping-poll instance. The polling instance no longer sends ICMP echo requests to the polled device. This also resets all counters for this polling instance.

**Syntax**    active  
             no active

**Mode**     Ping-Polling Configuration

**Examples** To activate the ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# active
```

To disable the ping-poll instance 43 and reset its counters, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no active
```

**Related commands**    [debug ping-poll](#)  
                      [ip \(ping-polling\)](#)  
                      [ping-poll](#)  
                      [show ping-poll](#)

# clear ping-poll

**Overview** This command resets the specified ping poll, or all ping poll instances. This clears the ping counters, and changes the status of polled devices to unreachable. The polling instance changes to the polling frequency specified with the [critical-interval](#) command. The device status changes to reachable once the device responses have reached the [up-count](#).

**Syntax** `clear ping-poll {<1-100>|all}`

| Parameter | Description                                                                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-100>   | A ping poll ID number. The specified ping poll instance has its counters cleared, and the status of the device it polls is changed to unreachable. |
| all       | Clears the counters and changes the device status of all polling instances.                                                                        |

**Mode** Privileged Exec

**Examples** To reset the ping poll instance 12, use the command:

```
awplus# clear ping-poll 12
```

To reset all ping poll instances, use the command:

```
awplus# clear ping-poll all
```

**Related commands** [active \(ping-polling\)](#)  
[ping-poll](#)  
[show ping-poll](#)

# critical-interval

**Overview** This command specifies the time period in seconds between pings when the polling instance has not received a reply to at least one ping, and when the device is unreachable.

This command enables the device to quickly observe changes in state, and should be set to a much lower value than the [normal-interval](#) command.

The **no** variant of this command sets the critical interval to the default of one second.

**Syntax** `critical-interval <1-65536>`  
`no critical-interval`

| Parameter | Description                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------|
| <1-65536> | Time in seconds between pings, when the device has failed to a ping, or the device is unreachable. |

**Default** The default is 1 second.

**Mode** Ping-Polling Configuration

**Examples** To set the critical interval to 2 seconds for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# critical-interval 2
```

To reset the critical interval to the default of one second for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# no critical-interval
```

**Related commands** [fail-count](#)  
[normal-interval](#)  
[sample-size](#)  
[show ping-poll](#)  
[timeout \(ping polling\)](#)  
[up-count](#)



# debug ping-poll

**Overview** This command enables ping poll debugging for the specified ping-poll instance. This generates detailed messages about ping execution.

The **no** variant of this command disables ping-poll debugging for the specified ping-poll.

**Syntax** `debug ping-poll <1-100>`  
`no debug ping-poll {<1-100>|all}`

| Parameter | Description                       |
|-----------|-----------------------------------|
| <1-100>   | A unique ping poll ID number.     |
| all       | Turn off all ping-poll debugging. |

**Mode** Privileged Exec

**Examples** To enable debugging for ping-poll instance 88, use the command:

```
awplus# debug ping-poll 88
```

To disable all ping poll debugging, use the command:

```
awplus# no debug ping-poll all
```

To disable debugging for ping-poll instance 88, use the command:

```
awplus# no debug ping-poll 88
```

**Related commands** [active \(ping-polling\)](#)  
[clear ping-poll](#)  
[ping-poll](#)  
[show ping-poll](#)  
[undebug ping-poll](#)

## description (ping-polling)

**Overview** This command specifies a string to describe the ping-polling instance. This allows the ping-polling instance to be recognized easily in show commands. Setting this command is optional.

By default ping-poll instances do not have a description.

Use the **no** variant of this command to delete the description set.

**Syntax** `description <description>`  
`no description`

| Parameter                        | Description                                                                                                                   |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;description&gt;</code> | The description of the target. Valid characters are any printable character and spaces. There is no maximum character length. |

**Mode** Ping-Polling Configuration

**Examples** To add the text "Primary Gateway" to describe the ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# description Primary Gateway
```

To delete the description set for the ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no description
```

**Related commands** [ping-poll](#)  
[show ping-poll](#)

# fail-count

**Overview** This command specifies the number of pings that must be unanswered, within the total number of pings specified by the [sample-size](#) command, for the ping-polling instance to consider the device unreachable.

If the number set by the [sample-size](#) command and the **fail-count** commands are the same, then the unanswered pings must be consecutive. If the number set by the [sample-size](#) command is greater than the number set by the **fail-count** command, then a device that does not always reply to pings may be declared unreachable.

The **no** variant of this command resets the fail count to the default.

**Syntax** `fail-count <1-100>`  
`no fail-count`

| Parameter                  | Description                                                                                                                        |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;1-100&gt;</code> | The number of pings within the sample size that a reachable device must fail to respond to before it is classified as unreachable. |

**Default** The default is 5.

**Mode** Ping-Polling Configuration

**Examples** To specify the number of pings that must fail within the sample size to determine that a device is unreachable for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# fail-count 5
```

To reset the fail-count to its default of 5 for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no fail-count
```

**Related commands**

- [critical-interval](#)
- [normal-interval](#)
- [ping-poll](#)
- [sample-size](#)
- [show ping-poll](#)
- [timeout \(ping polling\)](#)
- [up-count](#)

# ip (ping-polling)

**Overview** This command specifies the IPv4 address of the device you are polling.

**Syntax** `ip {<ip-address>|<ipv6-address>}`

| Parameter                         | Description                                        |
|-----------------------------------|----------------------------------------------------|
| <code>&lt;ip-address&gt;</code>   | An IPv4 address in dotted decimal notation A.B.C.D |
| <code>&lt;ipv6-address&gt;</code> | An IPv6 address in hexadecimal notation X:X::X:X   |

**Mode** Ping-Polling Configuration

**Examples** To set ping-poll instance 5 to poll the device with the IP address 192.168.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 5
awplus(config-ping-poll)# ip 192.168.0.1
```

To set ping-poll instance 10 to poll the device with the IPv6 address 2001:db8::, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 10
awplus(config-ping-poll)# ip 2001:db8::
```

**Related commands**

- [ping-poll](#)
- [source-ip](#)
- [show ping-poll](#)

# length (ping-poll data)

**Overview** This command specifies the number of data bytes to include in the data portion of the ping packet. This allows you to set the ping packets to a larger size if you find that larger packet types in your network are not reaching the polled device, while smaller packets are getting through. This encourages the polling instance to change the device's status to unreachable when the network is dropping packets of the size you are interested in.

The **no** variant of this command resets the data bytes to the default of 32 bytes.

**Syntax** `length <4-1500>`  
`no length`

| Parameter                   | Description                                                                 |
|-----------------------------|-----------------------------------------------------------------------------|
| <code>&lt;4-1500&gt;</code> | The number of data bytes to include in the data portion of the ping packet. |

**Default** The default is 32.

**Mode** Ping-Polling Configuration

**Examples** To specify that ping-poll instance 12 sends ping packet with a data portion of 56 bytes, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 12
awplus(config-ping-poll)# length 56
```

To reset the number of data bytes in the ping packet to the default of 32 bytes for ping-poll instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 12
awplus(config-ping-poll)# length
```

**Related commands** [ping-poll](#)  
[show ping-poll](#)

# normal-interval

**Overview** This command specifies the time period between pings when the device is reachable.

The **no** variant of this command resets the time period to the default of 30 seconds.

**Syntax** `normal-interval <1-65536>`  
`no normal-interval`

| Parameter                    | Description                                                 |
|------------------------------|-------------------------------------------------------------|
| <code>&lt;1-65536&gt;</code> | Time in seconds between pings when the target is reachable. |

**Default** The default is 30 seconds.

**Mode** Ping-Polling Configuration

**Examples** To specify a time period of 60 seconds between pings when the device is reachable for ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# normal-interval 60
```

To reset the interval to the default of 30 seconds for ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no normal-interval
```

**Related commands**

- [critical-interval](#)
- [fail-count](#)
- [ping-poll](#)
- [sample-size](#)
- [show ping-poll](#)
- [timeout \(ping polling\)](#)
- [up-count](#)

# ping-poll

**Overview** This command enters the ping-poll configuration mode. If a ping-poll exists with the specified number, then this command enters its configuration mode. If no ping-poll exists with the specified number, then this command creates a new ping poll with this ID number.

To configure a ping-poll, create a ping poll using this command, and use the [ip \(ping-polling\)](#) command to specify the device you want the polling instance to poll. It is not necessary to specify any further commands unless you want to change a command's default.

The **no** variant of this command deletes the specified ping poll.

**Syntax** `ping-poll <1-100>`  
`no ping-poll <1-100>`

| Parameter                  | Description                   |
|----------------------------|-------------------------------|
| <code>&lt;1-100&gt;</code> | A unique ping poll ID number. |

**Mode** Global Configuration

**Examples** To create ping-poll instance 3 and enter ping-poll configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 3
awplus(config-ping-poll)#
```

To delete ping-poll instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# no ping-poll 3
```

**Related commands**

- [active \(ping-polling\)](#)
- [clear ping-poll](#)
- [debug ping-poll](#)
- [description \(ping-polling\)](#)
- [ip \(ping-polling\)](#)
- [length \(ping-poll data\)](#)
- [show ping-poll](#)
- [source-ip](#)

# sample-size

**Overview** This command sets the total number of pings that the polling instance inspects when determining whether a device is unreachable. If the number of pings specified by the **fail-count** command go unanswered within the inspected sample, then the device is declared unreachable.

If the numbers set in this command and **fail-count** command are the same, the unanswered pings must be consecutive. If the number set by this command is greater than that set with the **fail-count** command, a device that does not always reply to pings may be declared unreachable.

You cannot set this command's value lower than the **fail-count** value.

The polling instance uses the number of pings specified by the **up-count** command to determine when a device is reachable.

The **no** variant of this command resets this command to the default.

**Syntax** `sample-size <1-100>`  
`no sample size`

| Parameter | Description                                             |
|-----------|---------------------------------------------------------|
| <1-100>   | Number of pings that determines critical and up counts. |

**Default** The default is 5.

**Mode** Ping-Polling Configuration

**Examples** To set the sample-size to 50 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# sample-size 50
```

To reset sample-size to the default of 5 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no sample-size
```



**Related  
commands**

- [critical-interval](#)
- [fail-count](#)
- [normal-interval](#)
- [ping-poll](#)
- [show ping-poll](#)
- [timeout \(ping polling\)](#)
- [up-count](#)

# show counter ping-poll

**Overview** This command displays the counters for ping polling.

**Syntax** `show counter ping-poll [<1-100>]`

| Parameter | Description                                                                                                                                                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-100>   | A unique ping poll ID number. This displays the counters for the specified ping poll only. If you do not specify a ping poll, then this command displays counters for all ping polls. |

**Mode** User Exec and Privileged Exec

**Output** Figure 53-1: Example output from the **show counter ping-poll** command

|                       |          |
|-----------------------|----------|
| Ping-polling counters |          |
| Ping-poll: 1          |          |
| PingsSent             | ..... 15 |
| PingsFailedUpState    | ..... 0  |
| PingsFailedDownState  | ..... 0  |
| ErrorSendingPing      | ..... 2  |
| CurrentUpCount        | ..... 13 |
| CurrentFailCount      | ..... 0  |
| UpStateEntered        | ..... 0  |
| DownStateEntered      | ..... 0  |
| Ping-poll: 2          |          |
| PingsSent             | ..... 15 |
| PingsFailedUpState    | ..... 0  |
| PingsFailedDownState  | ..... 0  |
| ErrorSendingPing      | ..... 2  |
| CurrentUpCount        | ..... 13 |
| CurrentFailCount      | ..... 0  |
| UpStateEntered        | ..... 0  |
| DownStateEntered      | ..... 0  |
| Ping-poll: 5          |          |
| PingsSent             | ..... 13 |
| PingsFailedUpState    | ..... 0  |
| PingsFailedDownState  | ..... 2  |
| ErrorSendingPing      | ..... 2  |
| CurrentUpCount        | ..... 9  |
| CurrentFailCount      | ..... 0  |
| UpStateEntered        | ..... 0  |
| DownStateEntered      | ..... 0  |

**Table 54:** Parameters in output of the **show counter ping-poll** command

| Parameter            | Description                                                                                                                                                  |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ping-poll            | The ID number of the polling instance.                                                                                                                       |
| PingsSent            | The total number of pings generated by the polling instance.                                                                                                 |
| PingsFailedUpState   | The number of unanswered pings while the target device is in the Up state. This is a cumulative counter for multiple occurrences of the Up state.            |
| PingsFailedDownState | Number of unanswered pings while the target device is in the Down state. This is a cumulative counter for multiple occurrences of the Down state.            |
| ErrorSendingPing     | The number of pings that were not successfully sent to the target device.<br>This error can occur when your device does not have a route to the destination. |
| CurrentUpCount       | The current number of sequential ping replies.                                                                                                               |
| CurrentFailCount     | The number of ping requests that have not received a ping reply in the current sample-size window.                                                           |
| UpStateEntered       | Number of times the target device has entered the Up state.                                                                                                  |
| DownStateEntered     | Number of times the target device has entered the Down state.                                                                                                |

**Example** To display counters for the polling instances, use the command:

```
awplus# show counter ping-poll
```

**Related commands**

- [debug ping-poll](#)
- [ping-poll](#)
- [show ping-poll](#)

# show ping-poll

**Overview** This command displays the settings and status of ping polls.

**Syntax** `show ping-poll [<1-100>|state {up|down}] [brief]`

| Parameter | Description                                                                                                    |
|-----------|----------------------------------------------------------------------------------------------------------------|
| <1-100>   | Displays settings and status for the specified polling instance.                                               |
| state     | Displays polling instances based on whether the device they are polling is currently reachable or unreachable. |
|           | up Displays polling instance where the device state is reachable.                                              |
|           | down Displays polling instances where the device state is unreachable.                                         |
| brief     | Displays a summary of the state of ping polls, and the devices they are polling.                               |

**Mode** User Exec and Privileged Exec

**Output** Figure 53-2: Example output from the **show ping-poll brief** command

|                         |         |       |               |
|-------------------------|---------|-------|---------------|
| Ping Poll Configuration |         |       |               |
| -----                   |         |       |               |
| Id                      | Enabled | State | Destination   |
| -----                   |         |       |               |
| 1                       | Yes     | Down  | 192.168.0.1   |
| 2                       | Yes     | Up    | 192.168.0.100 |

**Table 55:** Parameters in output of the **show ping-poll brief** command

| Parameter | Meaning                                                                                                                   |
|-----------|---------------------------------------------------------------------------------------------------------------------------|
| Id        | The ID number of the polling instance, set when creating the polling instance with the <a href="#">ping-poll</a> command. |
| Enabled   | Whether the polling instance is enabled or disabled.                                                                      |

**Table 55:** Parameters in output of the **show ping-poll brief** command (cont.)

| Parameter     | Meaning                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------|
| State         | The current status of the device being polled:                                                                                           |
| Up            | The device is reachable.                                                                                                                 |
| Down          | The device is unreachable.                                                                                                               |
| Critical Up   | The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down.    |
| Critical Down | The device is unreachable but the polling instance received a reply to the last ping packet, so the polled device may be coming back up. |
| Destination   | The IP address of the polled device, set with the <a href="#">ip (ping-polling)</a> command.                                             |

**Figure 53-3:** Example output from the **show ping-poll** command

```

Ping Poll Configuration

Poll 1:
Description : Primary Gateway
Destination IP address : 192.168.0.1
Status : Down
Enabled : Yes
Source IP address : 192.168.0.10
Critical interval : 1
Normal interval : 30
Fail count : 10
Up count : 5
Sample size : 50
Length : 32
Timeout : 1
Debugging : Enabled

```

|                        |                     |
|------------------------|---------------------|
| Poll 2:                |                     |
| Description            | : Secondary Gateway |
| Destination IP address | : 192.168.0.100     |
| Status                 | : Up                |
| Enabled                | : Yes               |
| Source IP address      | : Default           |
| Critical interval      | : 5                 |
| Normal interval        | : 60                |
| Fail count             | : 20                |
| Up count               | : 30                |
| Sample size            | : 100               |
| Length                 | : 56                |
| Timeout                | : 2                 |
| Debugging              | : Enabled           |

**Table 56:** Parameters in output of the **show ping-poll** command

| Parameter              | Description                                                                                                                                                                                                           |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Description            | Optional description set for the polling instance with the <a href="#">description (ping-polling)</a> command.                                                                                                        |
| Destination IP address | The IP address of the polled device, set with the <a href="#">ip (ping-polling)</a> command.                                                                                                                          |
| Status                 | The current status of the device being polled:                                                                                                                                                                        |
|                        | Up      The device is reachable.                                                                                                                                                                                      |
|                        | Down    The device is unreachable.                                                                                                                                                                                    |
|                        | Critical Up    The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down.                                                                  |
|                        | Critical Down    The device is unreachable but the polling instance received a reply to the last ping packet, so the polled device may be coming back up.                                                             |
| Enabled                | Whether the polling instance is enabled or disabled. The <a href="#">active (ping-polling)</a> and <a href="#">active (ping-polling)</a> commands enable and disable a polling instance.                              |
| Source IP address      | The source IP address sent in the ping packets. This is set using the <a href="#">source-ip</a> command.                                                                                                              |
| Critical interval      | The time period in seconds between pings when the polling instance has not received a reply to at least one ping, and when the device is unreachable. This is set with the <a href="#">critical-interval</a> command. |
| Normal interval        | The time period between pings when the device is reachable. This is set with the <a href="#">normal-interval</a> command.                                                                                             |

**Table 56:** Parameters in output of the **show ping-poll** command (cont.)

| Parameter   | Description                                                                                                                                                                                                                                                |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fail count  | The number of pings that must be unanswered, within the total number of pings specified by the <a href="#">sample-size</a> command, for the polling instance to consider the device unreachable. This is set using the <a href="#">fail-count</a> command. |
| Up count    | The number of consecutive pings that the polling instance must receive a reply to before classifying the device reachable again. This is set using the <a href="#">up-count</a> command.                                                                   |
| Sample size | The total number of pings that the polling instance inspects when determining whether a device is unreachable. This is set using the <a href="#">sample-size</a> command.                                                                                  |
| Length      | The number of data bytes to include in the data portion of the ping packet. This is set using the <a href="#">length (ping-poll data)</a> command.                                                                                                         |
| Timeout     | The time in seconds that the polling instance waits for a response to a ping packet. This is set using the <a href="#">timeout (ping polling)</a> command.                                                                                                 |
| Debugging   | Indicates whether ping polling debugging is <b>Enabled</b> or <b>Disabled</b> . This is set using the <a href="#">debug ping-poll</a> command.                                                                                                             |

**Examples** To display the ping poll settings and the status of all the polls, use the command:

```
awplus# show ping-poll
```

To display a summary of the ping poll settings, use the command:

```
awplus# show ping-poll brief
```

To display the settings for ping poll 6, use the command:

```
awplus# show ping-poll 6
```

To display a summary of the state of ping poll 6, use the command:

```
awplus# show ping-poll 6 brief
```

To display the settings of ping polls that have reachable devices, use the command:

```
awplus# show ping-poll state up
```

To display a summary of ping polls that have unreachable devices, use the command:

```
awplus# show ping-poll state down brief
```

**Related commands** [debug ping-poll](#)  
[ping-poll](#)

# source-ip

**Overview** This command specifies the source IP address to use in ping packets.

By default, the polling instance uses the address of the interface through which it transmits the ping packets. It uses the device's local interface IP address when it is set. Otherwise, the IP address of the interface through which it transmits the ping packets is used.

The **no** variant of this command resets the source IP in the packets to the device's local interface IP address.

**Syntax** `source-ip {<ip-address>|<ipv6-address>}`  
`no source-ip`

| Parameter                         | Description                                        |
|-----------------------------------|----------------------------------------------------|
| <code>&lt;ip-address&gt;</code>   | An IPv4 address in dotted decimal notation A.B.C.D |
| <code>&lt;ipv6-address&gt;</code> | An IPv6 address in hexadecimal notation X:X::X:X   |

**Mode** Ping-Polling Configuration

**Examples** To configure the ping-polling instance 43 to use the source IP address 192.168.0.1 in ping packets, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# source-ip 192.168.0.1
```

To configure the ping-polling instance 43 to use the source IPv6 address 2001:db8:: in ping packets, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# source-ip 2001:db8::
```

To reset the source IP address to the device's local interface IP address for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no source-ip
```



**Related commands**

- description (ping-polling)
- ip (ping-polling)
- length (ping-poll data)
- ping-poll
- show ping-poll

# timeout (ping polling)

**Overview** This command specifies the time in seconds that the polling instance waits for a response to a ping packet. You may find a higher time-out useful in networks where ping packets have a low priority.

The **no** variant of this command resets the set time out to the default of one second.

**Syntax** `timeout <1-30>`  
`no timeout`

| Parameter | Description                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------|
| <1-30>    | Length of time, in seconds, that the polling instance waits for a response from the polled device. |

**Default** The default is 1 second.

**Mode** Ping-Polling Configuration

**Examples** To specify the timeout as 5 seconds for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# timeout 5
```

To reset the timeout to its default of 1 second for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no timeout
```

**Related commands** [critical-interval](#)  
[fail-count](#)  
[normal-interval](#)  
[ping-poll](#)  
[sample-size](#)  
[show ping-poll](#)  
[up-count](#)

# up-count

**Overview** This command sets the number of consecutive pings that the polling instance must receive a reply to before classifying the device reachable again.

The **no** variant of this command resets the up count to the default of 30.

**Syntax** `up-count <1-100>`  
`no up-count`

| Parameter                  | Description                                                                      |
|----------------------------|----------------------------------------------------------------------------------|
| <code>&lt;1-100&gt;</code> | Number of replied pings before an unreachable device is classified as reachable. |

**Default** The default is 30.

**Mode** Ping-Polling Configuration

**Examples** To set the upcount to 5 consecutive pings for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# up-count 5
```

To reset the upcount to the default value of 30 consecutive pings for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no up-count
```

**Related commands**

- [critical-interval](#)
- [fail-count](#)
- [normal-interval](#)
- [ping-poll](#)
- [sample-size](#)
- [show ping-poll](#)
- [timeout \(ping polling\)](#)

# undebbug ping-poll

**Overview** This command applies the functionality of the no [debug ping-poll](#) command.

## Introduction

**Overview** This chapter provides an alphabetical reference for sFlow commands.  
For more information, see the [sFlow Feature Overview and Configuration Guide](#).

- Command List**
- “[debug sflow](#)” on page 2506
  - “[debug sflow agent](#)” on page 2507
  - “[sflow agent](#)” on page 2508
  - “[sflow collector](#)” on page 2510
  - “[sflow collector id](#)” on page 2511
  - “[sflow collector max-datagram-size](#)” on page 2513
  - “[sflow enable](#)” on page 2514
  - “[sflow max-header-size](#)” on page 2515
  - “[sflow polling-interval](#)” on page 2517
  - “[sflow sampling-rate](#)” on page 2518
  - “[show debugging sflow](#)” on page 2519
  - “[show running-config sflow](#)” on page 2520
  - “[show sflow](#)” on page 2521
  - “[show sflow interface](#)” on page 2523
  - “[undebug sflow](#)” on page 2524

# debug sflow

**Overview** This command enables sFlow® debug message logging, for sFlow sampling and polling activity on the specified ports. If no ports are specified, sampling and/or polling debug messages are enabled for all ports.

The **no** variant of this command disables sFlow sampling and or polling debug message logging on the ports selected. If no ports are specified, sampling and/or polling debug messages are disabled on all ports.

**Syntax** debug sflow [interface <port-list>] [sampling][polling]  
no debug sflow [interface <port-list>] [sampling][polling]

| Parameter | Description                                     |
|-----------|-------------------------------------------------|
| interface | Interface information.                          |
| sampling  | Debug sFlow sampling for the specified port(s). |
| polling   | Debug sFlow polling for the specified port(s).  |

**Default** The sFlow sampling and or polling debug is disabled.

**Mode** Privileged Exec

**Examples** To enable logging and polling of sFlow debug messages for polling and sampling on all ports, use the command:

```
awplus# debug sflow sampling polling
```

**Related commands** [show debugging sflow](#)  
[no debug all](#)

# debug sflow agent

**Overview** This command enables sFlow® debug message logging that is not specific to particular ports. For example, sending an sFlow datagram to the collector.

The **no** variant of this command applies the command default.

**Syntax** debug sflow agent  
no debug sflow agent

**Default** The sFlow agent debug message logging (that is not port specific) is disabled.

**Mode** Privileged Exec

**Example** To enable logging of sFlow agent debug messages, use the following command:

```
awplus# debug sflow agent
```

**Related commands** [show debugging sflow](#)  
[debug sflow](#)

# sflow agent

**Overview** This command sets the sFlow® agent IP address on the switch. This address is inserted into every sFlow datagram sent from the sFlow agent switch to the sFlow collector device. The sFlow collector can then use this address to uniquely identify and to access the switch, such as for SNMP. We therefore recommend that you change this address as little as possible.

Although the agent address can be set to any valid IPv4 or IPv6 address; we recommended that you set the sFlow® agent IP address to be the **local address** that is configured on the switch. For information on local addresses and how to set them up, see the [interface \(to configure\)](#) command. This ensures that the sFlow collector can maintain connectivity to the switch irrespective of the addition or deletion of interfaces (each of which will have its own specific IP address). Note that sFlow is rendered inactive whenever the agent address is not set.

The **no** variant of this command applies its default setting to remove a configured address.

**Syntax** `sflow agent {ip <ip-address>|ipv6 <ipv6-address>}`  
`no sflow agent {ip|ipv6}`

| Parameter      | Description                                                                                                  |
|----------------|--------------------------------------------------------------------------------------------------------------|
| <ip-address>   | The IPv4 address of the switch that is acting as the sFlow agent.                                            |
| <ipv6-address> | The IPv6 address of the switch that is acting as the sFlow agent. The IPv6 address uses the format X:X::X:X. |

**Default** The sFlow agent address is unset.

**Mode** Global Configuration

**Examples** To set the sFlow agent (IPv4) address to 192.0.2.23, use the command:

```
awplus# configure terminal
awplus(config)# sflow agent ip 192.0.2.23
```

To remove the sFlow agent (IPv4) address, use the command:

```
awplus# configure terminal
awplus(config)# no sflow agent ip
```

To set the sFlow agent (IPv6) address to 2001:0db8::1, use the command:

```
awplus# configure terminal
awplus(config)# sflow agent ipv6 2001:0db8::1
```

To remove the sFlow agent (IPv6) address, use the command:

```
awplus# configure terminal
awplus(config)# no sflow agent ipv6
```



**Related  
commands**    [show running-config sflow](#)  
                  [show sflow](#)

# sflow collector

**Overview** This command has been deprecated. It has been replaced by the [sflow collector id](#) command.

This command sets the sFlow® agent's collector IP address and/or UDP port.

**Command changes** Version 5.5.1-1.1: command deprecated.

# sflow collector id

**Overview** Use this command to set the sFlow® agent's collector IP address and optionally the port and maximum datagram size. This is the destination IP address and UDP port, for sFlow datagrams sent from the sFlow agent. The IP address can be any valid IPv4 or IPv6 address.

Use the **no** variant of this command to remove the configuration for that collector and render it inactive.

**Syntax** `sflow collector id <1-5> ip <ip-address> [port <1-65535>|max-datagram-size <200-1500>]`  
`sflow collector id <1-5> ipv6 <ipv6-address> [port <1-65535>|max-datagram-size <200-1500>]`  
`no sflow collector id <1-5>`

| Parameter         | Description                                                                                             |
|-------------------|---------------------------------------------------------------------------------------------------------|
| <ip-address>      | IPv4 address of the remote sFlow collector.                                                             |
| <ipv6-address>    | IPv6 address of remote sFlow collector.<br>The IPv6 address uses the format X:X::X:X.                   |
| port              | Destination UDP port for sFlow datagrams sent to the collector.                                         |
| <1-65535>         | UDP port number (default: 6343).                                                                        |
| max-datagram-size | The maximum number of bytes that can be sent in an sFlow datagram sent from the agent to the collector. |
| <200-1500>        | The value set for the max-datagram-size.                                                                |

**Default** By default the collector does not exist until configured with a valid IP address.

**Mode** Global Configuration

**Examples** To set the address of collector 1 to 192.168.1.36 with default port and max-datagram size, use the commands:

```
awplus# configure terminal
awplus(config)# sflow collector id 1 ip 192.168.1.36
```

To set the address of collector 2 to 12ae::213d::213d::333f and use UDP port 500, use the commands:

```
awplus# configure terminal
awplus(config)# sflow collector id 2 ipv6
12ae::213d::213d::333f port 500
```

To set the address of collector 5 to 10.42.2.70 and use UDP port 7777 and have a max-datagram-size of 800, use the commands:

```
awplus# configure terminal
awplus(config)# sflow collector id 5 ip 10.42.2.70 port 7777
max-datagram-size 800
```

To delete collector 5, use the commands:

```
awplus# configure terminal
awplus(config)# no sflow collector id 5
```

**Related commands**   [show running-config sflow](#)  
                          [show sflow](#)

**Command changes**   Version 5.5.1-1.1: command added.

# sflow collector max-datagram-size

**Overview** This command has been deprecated. It has been replaced by the [sflow collector id](#) command.

This command sets the maximum size of the sFlow® datagrams sent to the collector.

**Command changes** Version 5.5.1-1.1: command deprecated

# sflow enable

**Overview** This command enables sFlow® globally on the switch.

The **no** variant of this command disables sFlow globally on the switch.

Note that enabling sFlow does not automatically set its operational status to active. To activate sFlow the following conditions need to be met:

- sFlow is enabled.
- The sFlow agent address is set.
- The sFlow collector address is set to a valid (non zero) IPv4 or IPv6 address.
- Polling or sampling is enabled on the ports to be sampled or polled.

**Syntax** `sflow enable`  
`no sflow enable`

**Default** sFlow is disabled globally on the switch.

**Mode** Global Configuration

**Example** To enable sFlow operation, use the command:

```
awplus# configure terminal
awplus(config)# sflow enable
```

**Related commands** [show running-config sflow](#)  
[show sflow](#)

# sflow max-header-size

**Overview** This command sets the maximum header size of the Ethernet frames sampled on a specified port. The maximum header size is measured in bytes, referenced from the first byte of the Ethernet destination address and excludes the Ethernet FCS fields.

If a sampled Ethernet frame is longer than the maximum header size set by this command, then the frame will be truncated to the first N bytes before being placed in the sFlow datagram, where N is the maximum header size set by this command.

The **no** variant of this command resets the max-header-size to its default.

**Syntax** `sflow max-header-size <14-200>`  
`no sflow max-header-size`

| Parameter | Description                                       |
|-----------|---------------------------------------------------|
| <14-200>  | The maximum number of header bytes to be sampled. |

**Default** The max-header-size is 128 bytes.

**Mode** Interface Configuration

**Usage notes** The header size is measured from the first byte of the Ethernet frame MAC Destination Address.

- For an environment using standard TCP IPv4 over Ethernet frames, consider the following basic protocol structure:

Ethernet header (including the 4 byte 802.1Q header component) = 18 bytes

IPv4 header = 24 bytes

TCP header = 24 bytes

Total = 66 bytes

**CAUTION:** For IPv4, any data existing between 66 bytes and the value set by this command will be included in the sFlow packet samples. For example, with the default of 128 applied, up to 128-66=62 bytes of user data could be included in the sFlow datagram samples sent between the Agent and the Collector.

For more information, see the [sFlow Feature Overview and Configuration Guide](#).

- A similar consideration can be made for an environment using TCP IPv6 over Ethernet:

Ethernet header (including the 4 byte 802.1Q header component) = 18 bytes

IPv6 header = 40 bytes

TCP header = 24 bytes

Total = 82 bytes

**CAUTION:** For IPv6, any data existing between 82 bytes and the value set by this command will be included in the sFlow packet samples. For example, with the default of 128 applied, up to  $128-82=46$  bytes of user data could be included in the sFlow datagram samples sent between the Agent and the Collector.

Note that the agent-to-collector datagrams contain their own UDP headers, which are outside this calculation.

### Example

**Related commands** [show running-config sflow](#)  
[show sflow interface](#)  
[sflow max-header-size](#)



# sflow polling-interval

**Overview** This command sets the sFlow® counter polling interval (in seconds) for the specified ports. A value of 0 disables polling. A counter sample is taken every N seconds where N is the value set by this command.

The **no** variant of this command applies the default.

**Syntax** `sflow polling-interval {0|<1-16777215>}`  
`no sflow polling-interval`

| Parameter    | Description                      |
|--------------|----------------------------------|
| 0            | Disable polling (the default).   |
| <1-16777215> | The polling interval in seconds. |

**Default** The polling-interval is 0 (polling disabled).

**Mode** Interface Configuration

## Example

**Related commands** [show running-config sflow](#)  
[show sflow interface](#)

# sflow sampling-rate

**Overview** This command sets the mean sFlow® sampling rate for the specified ports. Sampling occurs every N frames (on average), where N is the rate value set via this command. The sampling rate applies to ingress and egress frames independently. For example, a value of 1000 will sample one frame in every 1000 frames received, i.e. one in every 1000 frames sent from the specified port. A value of 0 disables sampling on the specified port(s).

The **no** variant of this command applies the default.

**Syntax** `sflow sampling-rate <256-16777215>`  
`no sflow sampling-rate`

| Parameter      | Description                                       |
|----------------|---------------------------------------------------|
| <256-16777215> | The sampling rate N, measured in Ethernet frames. |

**Default** The sampling-rate is 0 (sampling disabled).

**Mode** Interface Configuration

**Example** To set the sampling rate to 500 for eth1 and eth2, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1,eth2
awplus(config-if)# sflow sampling-rate 500
```

**Related commands** [show running-config sflow](#)  
[show sflow interface](#)

# show debugging sflow

**Overview** This command displays sFlow® debug settings for agent operation, and for sampling and polling on specific interface ports. If no interface ports are specified, sampling and polling will be applied to all ports.

**Syntax** `show debugging sflow [interface <port-list>]`

| Parameter | Description                |
|-----------|----------------------------|
| interface | The interface information. |

**Mode** User Exec and Privileged Exec

## Example

**Output** Figure 54-1: Sample obtained for an sFlow agent  
To display sFlow debug settings for all ports, use the command:

```
awplus# show debugging sflow
```

**Related commands** [show running-config sflow](#)  
[show sflow interface](#)

# show running-config sflow

**Overview** This command displays the running system information specific to the sFlow feature.

**Syntax** `show running-config sflow`

**Mode** Privileged Exec and Global Configuration

**Example** To display the sFlow running configuration information, use the command:

```
awplus# show running-config sflow
```

**Output** Figure 54-2: Example output from the **show running-config sflow** command

**Related commands** [show running-config](#)

# show sflow

**Overview** This command displays non-port-specific sFlow agent configuration and operational status.

**Syntax** show sflow

**Mode** Privileged Exec

**Example** To display sFlow configuration and operational status, use the command:

```
awplus# show sflow
```

## Output

**Table 1:** Example output from the **show sflow** command

|                                            |                     |
|--------------------------------------------|---------------------|
| sFlow Agent Configuration:                 | Default Values      |
| sFlow Admin Status .....                   | Disabled [Disabled] |
| sFlow Agent Address .....                  | [not set] [not set] |
| Collector Address .....                    | 0.0.0.0 [0.0.0.0]   |
| Collector UDP Port .....                   | 6343 [6343]         |
| Tx Max Datagram Size .....                 | 1200 [1400]         |
| sFlow Agent Status:                        |                     |
| Polling/sampling/Tx .....                  |                     |
| Inactive because:                          |                     |
| - sFlow is disabled                        |                     |
| - Agent Addr is not set                    |                     |
| - Collector Addr is 0.0.0.0                |                     |
| - Polling & sampling disabled on all ports |                     |

**Table 2:** Parameters in the output of the **show sflow** command

| Output Parameter    | Description                                                                                                                                                    |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| sFlow Admin Status  | Whether sFlow agent operation is administratively enabled.                                                                                                     |
| sFlow Agent Address | The sFlow agent IPv4 or IPv6 address for the device. sFlow is rendered inactive whenever the agent address is not set.                                         |
| Collector Address   | The IPv4 or IPv6 collector address to which sFlow datagrams are sent. sFlow is rendered inactive whenever the collector address is set to 0.0.0.0 or 0:0::0.0. |
| Collector UDP Port  | The UDP port on the collector to which sFlow datagrams are sent.                                                                                               |

**Table 2:** Parameters in the output of the **show sflow** command (cont.)

| Output Parameter     | Description                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| Tx Max Datagram Size | The maximum size of the sFlow datagrams sent to the collector.                                                                |
| Polling/sampling/Tx  | Whether sFlow sampling and/or polling (and hence sFlow datagram transmission) are active. If inactive the reasons are listed. |

**Related commands** [show running-config sflow](#)  
[show sflow interface](#)

# show sflow interface

**Overview** This command displays sFlow agent sampling and polling configuration for all ports or a specified port.

**Syntax** `show sflow interface [<ifrang>]`

| Parameter | Description          |
|-----------|----------------------|
| <ifrang>  | The interface range. |

**Mode** Privileged Exec

**Example** To display the sFlow sampling and polling configuration for eth0, use the command:

```
awplus# show sflow interface eth0
```

**Output** Figure 54-3: Example output from the **show sflow interface** command

```
awplus#show sflow interface
```

|                           |                           |                     |                  |
|---------------------------|---------------------------|---------------------|------------------|
| sFlow Port Configuration: |                           |                     |                  |
| Default Values:           |                           |                     |                  |
|                           | Sampling Rate .....       | 0 pkts (= disabled) |                  |
|                           | Max Sample Header Size .. | 128 bytes           |                  |
|                           | Polling Interval .....    | 0 secs (= disabled) |                  |
|                           | Sampling Rate             | Max Header Size     | Polling Interval |
| Port                      | (1 in N pkts)             | (bytes)             | (secs)           |
| -----                     |                           |                     |                  |
| eth1                      | 0                         | 128                 | 0                |
| eth2                      | 0                         | 128                 | 0                |
| ...                       |                           |                     |                  |

**Related commands** [sflow enable](#)  
[show running-config sflow](#)  
[show sflow](#)

# undebug sflow

**Overview** This command applies the functionality of the **no** variant of the [debug sflow](#) command.



# **Part 8: Firewall and Network Address Translation (NAT)**

# 55

# Firewall Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure AlliedWare Plus Firewall. For more information see the [Firewall\\_and Network Address Translation \(NAT\) Feature Overview and Configuration\\_Guide](#).

The table below lists the firewall commands and their applicable modes.

Figure 55-1: Firewall commands and applicable modes

| Mode                   | Command                                      |
|------------------------|----------------------------------------------|
| Privileged Exec        | <code>clear firewall connections</code>      |
|                        | <code>debug firewall</code>                  |
|                        | <code>show debugging firewall</code>         |
|                        | <code>show firewall</code>                   |
|                        | <code>show firewall connections</code>       |
|                        | <code>show firewall rule</code>              |
|                        | <code>show firewall rule config-check</code> |
|                        | <code>show running-config firewall</code>    |
| Global Configuration   | <code>firewall</code>                        |
| Firewall Configuration | <code>protect (firewall)</code>              |
|                        | <code>rule (firewall)</code>                 |
|                        | <code>move rule (firewall)</code>            |

- Command List**
- “[clear firewall connections](#)” on page 2528
  - “[connection-limit \(firewall\)](#)” on page 2529
  - “[connection-log events](#)” on page 2531

- [“debug firewall”](#) on page 2532
- [“firewall”](#) on page 2533
- [“geoip update-interval”](#) on page 2534
- [“ip subnet dynamic geoip”](#) on page 2535
- [“ipv6 subnet dynamic geoip”](#) on page 2536
- [“ip tcp timeout established”](#) on page 2537
- [“move rule \(firewall\)”](#) on page 2538
- [“protect \(firewall\)”](#) on page 2539
- [“rule \(firewall\)”](#) on page 2540
- [“show connection-log events”](#) on page 2543
- [“show firewall”](#) on page 2544
- [“show firewall connections”](#) on page 2545
- [“show firewall connections limits”](#) on page 2546
- [“show firewall connections limits config-check”](#) on page 2547
- [“show firewall rule”](#) on page 2548
- [“show firewall rule config-check”](#) on page 2550
- [“show debugging firewall”](#) on page 2551
- [“show running-config firewall”](#) on page 2552

# clear firewall connections

**Overview** Use this command to clear firewall connections.

**Syntax** `clear firewall connections`

**Mode** Privileged Exec

**Usage notes** Removing the Network Address Translation (NAT) rule by using the **no nat rule** command for an actively translated flow does not stop translating immediately. This means subsequent packets in the flow are continued to be translated.

The continued translation after associated NAT rule is removed will only stop when:

- You use the **clear firewall connections** command to manually stop translations immediately, when the associated rule has been deleted regardless whether the firewall feature is actually configured with NAT or not.
- The traffic flow ends naturally, for example, when it is stopped from the source. If the flow is re-initiated from a host, it will not be translated by the firewall, as the rule is deleted after the first flow stopped.

**Examples** To clear firewall connections, use the command:

```
awplus# clear firewall connections
```

**Validation commands** [show firewall connections](#)

**Related commands** [rule \(nat\)](#)

# connection-limit (firewall)

**Overview** Use this command to limit firewall connections for an entity. The limit imposed by a connection-limit rule applies to the sum of TCP and UDP flows that match the rule.

You can use the tab key to auto-complete entity names.

Use the **no** variant of this command to remove the limit.

**Syntax** `connection-limit [<1-65535>] from <entity-name> with limit <0-100000>`  
`no connection-limit {<1-65535>|all}`

| Parameter     | Description                                                                                                                                                           |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-65535>     | Unique numeric identifier for the limit.                                                                                                                              |
| <entity-name> | An entity represents a logical grouping of subnets, hosts or interfaces. For more information about entity, see the <a href="#">Application and Entity Commands</a> . |
| <0-100000>    | The maximum number of permitted connections for the entity.                                                                                                           |
| all           | Delete all limits.                                                                                                                                                    |

**Default** The limiting is disabled by default and the number of connections will not be limited. However, the number is up to the maximum total number of allowed connections.

**Mode** Firewall Configuration

**Usage notes** This command allows you to limit the number of firewall sessions associated with a specific entity. The limit will be applied to each host on that entity. This means connection limits applied to an entity with multiple addresses will apply the limit to individual hosts, not the total connections for the entity. The limit applies to both IPv4 and IPv6.

If a connection limit rule is removed, any running connections are not stopped. Changes to limits only affect new connections. Adding a lower limit will not affect existing connections.

**Examples** To set a connection limit for entity DMZ, use the following command:

```
awplus(config-firewall)# connection-limit 1 from DMZ with limit 10000
```

To remove the connection limit, use the following command:

```
awplus(config-firewall)# no connection-limit 1
```

**Validation** `show firewall connections`  
**commands** `show firewall connections limits`

**Command** Version 5.5.0-1.1: Firewall session limiting rules apply to UDP connections, where  
**changes** previously the limiting rules only applied to TCP connections.

# connection-log events

**Overview** Use this command to enable extra logging for indicating the start and the end of connections passing through the firewall.

Use the **no** variant of this command to turn off the extra logging of connections passing through the firewall.

**Syntax** `connection-log events [new|end|all]`  
`no connection-log events [new|end|all]`

| Parameter | Description                                          |
|-----------|------------------------------------------------------|
| new       | New connection                                       |
| end       | Connections closed                                   |
| all       | All new connections and connections closed. Default. |

**Default** Connection logging is not enabled by default.

**Mode** Global Configuration.

**Usage notes** There are two types of messages you can log: new connections and connections that ended. You can control the amount of messages you log by choosing to log either type of message or all of the message types.

Messages contain the following information:

- time
- source and destination addresses (NATed and unNATed)
- protocol
- source and destination ports (NATed and unNATed)
- bytes and packets passed (found in the connection end message)

**Example** To log all of the new connections and all of the closed connections, use the commands:

```
awplus# configure terminal
awplus(config)# connection-log events all
```

**Related commands** [show connection-log events](#)

**Command changes** Version 5.4.7-1.1: command added.

# debug firewall

**Overview** Use this command to enable firewall debugging and Network Address Translation (NAT) debugging. This will cause additional detailed debugging information to be logged at the “informational” and “debugging” levels.

Use the **no** variant of this command to disable firewall debugging and NAT debugging.

For more information about NAT, see the [Firewall\\_and Network Address Translation \(NAT\) Feature Overview and Configuration\\_Guide](#).

**Syntax** `debug firewall`  
`no debug firewall`

**Default** Firewall debugging and NAT debugging are disabled by default.

**Mode** Privileged Exec

**Examples** To enable firewall debugging and NAT debugging, use the command:

```
awplus# debug firewall
```

To disable firewall debugging and NAT debugging, use the command:

```
awplus# no debug firewall
```

**Validation commands** [show debugging firewall](#)



# firewall

**Overview** Use this command to configure the firewall.  
Use the **no** variant of this command to remove all firewall configuration.

**Syntax** `firewall`  
`no firewall`

**Mode** Global Configuration

**Usage notes** This command allows you to enter the Firewall Configuration mode. The command prompt for this mode is **awplus(config-firewall)#**  
In the Firewall Configuration mode, you can:

- Enable or disable firewall protection, see the [protect \(firewall\)](#) command.
- Create, move, or delete rules for the firewall, see the [rule \(firewall\)](#) command and the [move rule \(firewall\)](#) command.

**Examples** To configure the firewall, use the commands:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)#
```

To remove all firewall configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no firewall
```

**Validation commands** [show firewall](#)  
[show running-config firewall](#)

# geoip update-interval

**Overview** Use this command to configure how often the GeoIP resource will be automatically downloaded from the Allied Telesis update server.

Use the **no** variant of this command to return to the default value of 24 hours.

**Syntax** `geoip update-interval {minutes <10-525600>|hours <1-8760>|days <1-365>|weeks <1-52>|never}`  
`no geoip update-interval`

| Parameter           | Description                                     |
|---------------------|-------------------------------------------------|
| minutes <10-525600> | Update interval from 10 through 52600 minutes.  |
| hours <1-8760>      | Update interval from 1 hour through 8760 hours. |
| days <1-365>        | Update interval from 1 day through 365 days.    |
| weeks <1-52>        | Update interval from 1 week through 52 weeks.   |
| never               | Never update the GeoIP resource.                |

**Default** 24 hours.

**Mode** Global Configuration

**Example** To configure the update interval of the GeoIP resource to 4 hours, use the commands:

```
awplus# configure terminal
awplus(config)# geoip update-interval hours 4
```

To return the update interval of the GeoIP resource to the default of 24 hours, use the commands:

```
awplus# configure terminal
awplus(config)# no geoip update-interval
```

**Related commands** [ipv6 subnet dynamic geoip](#)  
[ip subnet dynamic geoip](#)

**Command changes** Version 5.5.4-2.3: command added

# ip subnet dynamic geoip

**Overview** Use this command to create a network entity that will dynamically update with subnets from the GeoIP resource. This entity can then be used, for example, in Firewall rules to block traffic from a particular country.

Use the **no** variant of this command to remove a network entity that blocks traffic from a particular country.

**Syntax** `ip subnet dynamic geoip <country-code>`  
`no ip subnet dynamic geoip <country-code>`

| Parameter                         | Description           |
|-----------------------------------|-----------------------|
| <code>&lt;country-code&gt;</code> | ISO 3166 Country_Code |

**Mode** Network Configuration

**Usage notes** The GeoIP resource will be downloaded from the Allied Telesis updates server automatically. GeoIP networks are based on country of registration, not location, therefore the **accuracy of the data cannot be guaranteed**.

**Example** To configure an entity to block traffic to/from Russia, use the commands:

```
awplus# configure terminal
awplus(config)# zone russia
awplus(config-zone)# network geoip
awplus(config-network)# ip subnet dynamic geoip RU
```

To remove the entity that blocks traffic to/from Russia, use the commands:

```
awplus# configure terminal
awplus(config)# zone russia
awplus(config-zone)# network geoip
awplus(config-network)# no ip subnet dynamic geoip RU
```

**Related commands** [ipv6 subnet dynamic geoip](#)  
[geoip update-interval](#)

**Command changes** Version 5.5.4-2.2: command added

# ipv6 subnet dynamic geoip

**Overview** Use this command to create a network entity that will dynamically update with subnets from the GeoIP resource. This entity can then be used, for example, in Firewall rules to block traffic from a particular country.

Use the **no** variant of this command to remove a network entity that blocks traffic from a particular country.

**Syntax** `ipv6 subnet dynamic geoip <country-code>`  
`no ipv6 subnet dynamic geoip <country-code>`

| Parameter                         | Description           |
|-----------------------------------|-----------------------|
| <code>&lt;country-code&gt;</code> | ISO 3166 Country_Code |

**Mode** Network Configuration

**Usage notes** The GeoIP resource will be downloaded from the Allied Telesis updates server automatically. GeoIP networks are based on country of registration, not location, therefore the **accuracy of the data cannot be guaranteed**.

**Example** To configure an entity to block traffic to/from Russia, use the commands:

```
awplus# configure terminal
awplus(config)# zone russia
awplus(config-zone)# network geoip
awplus(config-network)# ipv6 subnet dynamic geoip RU
```

To remove the entity that blocks traffic to/from Russia, use the commands:

```
awplus# configure terminal
awplus(config)# zone russia
awplus(config-zone)# network geoip
awplus(config-network)# no ipv6 subnet dynamic geoip RU
```

**Related commands** [ip subnet dynamic geoip](#)  
[geoip update-interval](#)

**Command changes** Version 5.5.4-2.2: command added

# ip tcp timeout established

**Overview** Use this command to set the idle timeout for all established TCP connections.

Use the **no** variant of this command to set the idle timeout back to the default of 3600 seconds.

**Syntax** `ip tcp timeout established <1-31536000>`  
`no ip tcp timeout established`

| Parameter                       | Description                                                                |
|---------------------------------|----------------------------------------------------------------------------|
| <code>&lt;1-31536000&gt;</code> | Idle timeout for established TCP connections in seconds from 1 to 3153600. |

**Default** 3600 seconds (1 hour)

**Mode** Global Configuration

**Usage notes** By default, when a TCP session is successfully established through the firewall, when the session goes idle, it automatically times out of the firewall connection tracking table after 3600 seconds. In some situations it may be beneficial to time out unused established TCP sessions earlier.

For example, in a busy environment where there is an excessive number of sessions being established, the firewall connection tracking table could become oversubscribed, with new connections being blocked until older sessions are timed out.

**Example** To set a non-default TCP session timeout for established idle sessions of 1800 seconds (30 minutes), use the commands:

```
awplus# configure terminal
awplus(config)# ip tcp timeout established 1800
```

**Example** To set the TCP session timeout for established idle sessions back to the default setting of 3600 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip tcp timeout established
```

**Related commands** [show running-config](#)

**Command changes** Version 5.4.6-1.1: command added

# move rule (firewall)

**Overview** Use this command to change the order of firewall rules.

Firewall rules are applied in rule ID order. When rules match the same application, source entity and destination entity, only the rule with the lowest ID is applied.

Note that you can move an existing rule ID only to an ID that is not assigned to any rule; otherwise you will be given an error message. Also note that a change to the rule order may change the rule results.

**Syntax** `move rule <1-65535> to <1-65535>`

| Parameter                                  | Description                                                                                                                                                                                                                          |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>move rule<br/>&lt;1-65535&gt;</code> | Move the ID of a given rule. The rule ID of the given rule must exist.<br>Each rule has an ID which is either designated by the user or automatically generated when the rule is created. The rule ID is an integer from 1 to 65535. |
| <code>to &lt;1-65535&gt;</code>            | New rule ID to assign. The new rule ID must not be used by any existing rule.                                                                                                                                                        |

**Mode** Firewall Configuration

**Examples** To change the rule ID from 20 to 10, use the commands:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# move rule 20 to 10
```

**Validation commands** [show firewall rule](#)  
[show running-config firewall](#)

**Related commands** [rule \(firewall\)](#)

# protect (firewall)

**Overview** Use this command to enable firewall protection.

Use the **no** variant of this command to disable firewall protection without losing the existing firewall configuration.

**Syntax** `protect`  
`no protect`

**Default** Firewall protection is disabled by default.

**Mode** Firewall Configuration

**Usage notes** Firewall protection is disabled by default and all traffic can pass through the firewall. When the firewall is enabled and no rules are added, all traffic will be blocked by default. You can use the [rule \(firewall\)](#) command to configure rules to allow traffic to pass through the firewall.

**Examples** To enable firewall protection, use the commands:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# protect
```

To disable firewall protection, use the commands:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# no protect
```

**Validation commands** [show firewall](#)  
[show running-config firewall](#)

# rule (firewall)

**Overview** Use this command to create a rule for the firewall. Firewall security policy is specified in the form of firewall rules. Each rule defines the appropriate processing of a type of traffic passing through the firewall.

Use the **no** variant of this command to remove a rule.

**Syntax** rule [<1-65535>] {permit|deny|reject|log} <application-name>  
from <source-entity> to <destination-entity>  
[no-state-enforcement] [log]  
  
no rule {<1-65535>|all}

| Parameter          | Description                                                                                                                                                                                                                                                                                     |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-65535>          | Rule ID is an integer in the range <1-65535>. If you don't designate a rule ID, a rule ID will be automatically generated and it will be greater than the current highest rule ID.                                                                                                              |
| permit             | Permit connections that match the application, source entity and destination entity specified with this command.                                                                                                                                                                                |
| deny               | Drop connections that match the application, source entity and destination entity specified with this command. No error message is sent back to the source host.                                                                                                                                |
| reject             | Reject connections that match the application, source entity and destination entity specified with this command. An error message (for instance, a TCP reset for a rejected TCP connection, or a destination unreachable message for an ICMP connection, etc.) is sent back to the source host. |
| log                | When 'log' is the action for the rule, log an event each time the rule is hit. The traffic will also be processed by subsequent firewall rules which may permit, deny or reject the connection.                                                                                                 |
| <application-name> | Application name. You can either specify an application name or use the word <b>any</b> , which stands for all applications. For more information about applications, see Application and Entity Commands. You can use the tab key to auto-complete application names.                          |



| Parameter                               | Description                                                                                                                                                                                                                                                                                                   |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;source-entity&gt;</code>      | Source entity name. An entity represents a logical grouping of subnets, hosts or interfaces. For more information about entities, see Application and Entity Commands. You can use the tab key to auto-complete entity names.                                                                                 |
| <code>&lt;destination-entity&gt;</code> | Destination entity name.                                                                                                                                                                                                                                                                                      |
| <code>no-state-enforcement</code>       | Optionally disable state enforcement for this rule. Use this option with caution as it will allow reverse path connection initiation. It should be used only when the traffic forward and reverse paths must be different and there is no alternative approach available. This option is disabled by default. |
| <code>log</code>                        | When 'log' is appended to a rule, the action is applied and a log message is also generated each time the rule is hit.                                                                                                                                                                                        |
| <code>all</code>                        | Delete all rules.                                                                                                                                                                                                                                                                                             |

**Mode** Firewall Configuration

**Usage notes** When the firewall is enabled and no rules are added, all traffic is blocked by default, you can use this command to create rules for permitting packets between entities.

The rule is not valid and cannot be hit if either the application, source entity or destination entity the rule applies to is not properly configured, for example, the application does not exist or does not have a protocol configured or the entity does not exist. To configure applications and entities, see Application and Entity Commands. You can also use the [show firewall rule config-check](#) command to check rule configuration validity.

You can change the rule order by using the [move rule \(firewall\)](#) command.

**Examples** To create a rule for permitting application ping between 'public' and 'private', use the command:

```
awplus(config-firewall)# rule 10 permit
ping from public to private
```

To create a rule for denying application http between 'public.wan' and 'private.lan', use the command:

```
awplus(config-firewall)# rule 20 deny
http from public.wan to private.lan
```

To create a firewall rule to permit application 'ping' between 'public' and 'dmz' entities and to log the results, use the commands:

```
awplus(config-firewall)# rule 30 permit
ping from public to dmz log
```

**Related commands**    `move rule (firewall)`  
                          `show firewall rule`  
                          `show firewall rule config-check`

**Command changes**    Version 5.4.7-0.1: **no-state-enforcement** option added.

# show connection-log events

**Overview** This command displays the configuration state (enabled or disabled) for the logging of connections passing through the firewall, as configured by the [connection-log events](#) command.

**Syntax** `show connection-log events`

**Mode** User Exec

**Example** To show the logging configuration state for the connections passing through the firewall, use the command:

```
awplus# show connection-log events
```

**Output** Figure 55-2: Example output from **show connection-log events**

```
awplus#show connection-log events
Log new connection events: Disabled
Log connection end events: Enabled
```

**Related commands** [connection-log events](#)

**Command changes** Version 5.4.7-1.1: command added.

# show firewall

**Overview** Use this command to show the protection state of the firewall and the number of active connections being handled by the firewall.

You can use the [protect \(firewall\)](#) command to enable firewall protection.

**Syntax** `show firewall`

**Mode** Privileged Exec

**Examples** To show the state of the firewall, use the command:

```
awplus# show firewall
```

**Output** Figure 55-3: Example output from the **show firewall** command

```
awplus#show firewall
Firewall protection is enabled
Active connections: 9
```

**Related commands** [protect \(firewall\)](#)

# show firewall connections

**Overview** Use this command to show the connections currently being tracked by the firewall.

**Syntax** show firewall connections

**Mode** Privileged Exec

**Examples** To show the connections currently being tracked by the firewall, use the command:

```
awplus# show firewall connections
```

**Output** Figure 55-4: Example output from the **show firewall connections** command

```
awplus#show firewall connections
tcp ESTABLISHED src=192.168.1.2 dst=172.16.1.2 sport=58616
dport=23 packets=16
bytes=867 src=172.16.1.2 dst=172.16.1.1 sport=23 dport=58616
packets=11 bytes=636
[ASSURED]
icmpv6 src=2001:db8::2 dst=2001:db8::1 type=128 code=0 id=1416
packets=34
bytes=3536 src=2001:db8::1 dst=2001:db8::2 type=129 code=0 id=1416
packets=34
bytes=3536
tcp TIME_WAIT src=2001:db8:1::2 dst=2001:db8:2::2 sport=42532
dport=80 packets=7
bytes=597 src=2001:db8:2::2 dst=2001:db8:1::2 sport=80 dport=42532
packets=5
bytes=651 [ASSURED]
tcp TIME_WAIT src=2001:db8:1::2 dst=2001:db8:2::2 sport=48740
dport=80 packets=5
bytes=564 src=2001:db8:2::2 dst=2001:db8:1::2 sport=80 dport=48740
packets=5
bytes=594 [ASSURED]
```

**Related commands** [clear firewall connections](#)

# show firewall connections limits

**Overview** Use this command to show the configured firewall connection-limits for a given entity.

**Syntax** `show firewall connections limits`

**Mode** Privileged Exec

**Examples** To show the information about all the firewall connection limits, use the command:

```
awplus# show firewall connections limits
```

**Output** Figure 55-5: Example output from the **show firewall connections limits** command

| awplus#show firewall connections limits |        |       |           |
|-----------------------------------------|--------|-------|-----------|
| ID                                      | Entity | Limit | Hit Count |
| -----                                   |        |       |           |
| 10                                      | DMZ    | 100   | 42        |

**Related commands** [show firewall connections limits config-check](#)

# show firewall connections limits config-check

**Overview** Use this command to check configuration validity of firewall connection limits.

An invalid rule will not be active and cannot be hit. This command also shows the reasons why a limit configuration is not valid.

**Syntax** `show firewall connections limits config-check`

**Mode** Privileged Exec

**Usage notes** Firewall limits are applied to entities only. A limit is not valid if the source entity (zone) is not configured properly. This command checks if the entity exists at all, and if it does it also checks if the entity (zone) has a valid subnet.

**Examples** To check configuration validity of connection-limit rules, use the command:

```
awplus# show firewall connections limits
config-check
```

**Output** Figure 55-6: Example output from the **show firewall connections limits config-check** command on the console if rule configuration errors are detected. Connection-limit 10 uses an entity that exists; however no subnet has been specified. Connection-limit 20 uses an entity that doesn't exist.

```
awplus#show firewall connections limits config-check
Connection-limit 10:
 "From" entity has no subnet or host addresses
Connection-limit 20:
 "From" entity does not exist
```

**Output** Figure 55-7: Example output from the **show firewall connections limits config-check** command if all limit rules are valid

```
awplus#show firewall connection limits config-check
All rules are valid
```

**Related commands** [show firewall connections limits](#)

# show firewall rule

**Overview** Use this command to show information about firewall rules.

**Syntax** `show firewall rule [<1-65535>]`

| Parameter | Description |
|-----------|-------------|
| <1-65535> | Rule ID     |

**Mode** Privileged Exec

**Examples** To show information about all firewall rules, use the command:

```
awplus# show firewall rule
```

**Output** Figure 55-8: Example output from the **show firewall rule** command

```
awplus#show firewall rule
```

| [* = Rule is not valid - see "show firewall rule config-check"] |        |       |         |         |      |  |
|-----------------------------------------------------------------|--------|-------|---------|---------|------|--|
| ID                                                              | Action | App   | From    | To      | Hits |  |
| -----                                                           |        |       |         |         |      |  |
| 10                                                              | permit | ping  | public  | private | 0    |  |
| 20                                                              | permit | ping  | public  | dmz     | 0    |  |
| 40                                                              | permit | ping  | private | dmz     | 0    |  |
| * 50                                                            | permit | voice | public  | private | 0    |  |

To show information about a specific firewall rule, use the command:

```
awplus# show firewall rule 10
```

**Output** Figure 55-9: Example output from the **show firewall rule** command

```
awplus#show firewall rule 10
```

| [* = Rule is not valid - see "show firewall rule config-check"] |        |      |        |         |      |  |
|-----------------------------------------------------------------|--------|------|--------|---------|------|--|
| ID                                                              | Action | App  | From   | To      | Hits |  |
| -----                                                           |        |      |        |         |      |  |
| 10                                                              | permit | ping | public | private | 0    |  |

| Output Parameter | Description                                                                                                         |
|------------------|---------------------------------------------------------------------------------------------------------------------|
| *                | Indicates the rule is not valid and cannot be hit. See the <a href="#">show firewall rule config-check</a> command. |
| Action           | The rule action set by the <a href="#">rule (firewall)</a> command.                                                 |
| App              | Application name.                                                                                                   |



| Output Parameter | Description                                         |
|------------------|-----------------------------------------------------|
| From             | Source entity.                                      |
| To               | Destination entity.                                 |
| Hits             | The number of times the firewall rule has been hit. |

**Related commands** [rule \(firewall\)](#)

# show firewall rule config-check

**Overview** Use this command to check configuration validity of firewall rules.

An invalid rule will not be active and cannot be hit. This command also shows the reasons why a rule is not valid.

**Syntax** `show firewall rule config-check`

**Mode** Privileged Exec

**Usage notes** Firewall rules are applied to applications and entities. A rule is not valid if either the application, source entity or destination entity the rule applies to is not configured properly.

To configure applications and entities, see Application and Entity Commands.

**Examples** To check configuration validity of firewall rules, use the command:

```
awplus# show firewall rule config-check
```

**Output** Figure 55-10: Example output from the **show firewall rule config-check** command if rule configuration errors are detected

```
awplus#show firewall rule config-check
Rule 10:
 Application does not have a protocol configured
 "From" entity does not exist
 "To" entity has no subnet or host addresses
```

**Output** Figure 55-11: Example output from the **show firewall rule config-check** command if all rules are valid

```
awplus#show firewall rule config-check
All rules are valid
```

**Related commands** [rule \(firewall\)](#)  
[show firewall rule](#)

# show debugging firewall

**Overview** Use this command to see what debugging is turned on for firewall and Network Address Translation (NAT).  
You can use the [debug firewall](#) command to enable firewall and NAT debugging.  
For more information about NAT, see the [Firewall\\_and Network Address Translation \(NAT\) Feature Overview and Configuration\\_Guide](#).

**Syntax** show debugging firewall

**Mode** Privileged Exec

**Examples** To show the firewall and NAT debugging status, use the command:

```
awplus# show debugging firewall
```

**Output** Figure 55-12: Example output from the **show debugging firewall** command

```
awplus#show debugging firewall
Firewall Debugging Status: on
```

**Related commands** [debug firewall](#)

# show running-config firewall

**Overview** Use this command to show the configuration commands that have been used to configure the firewall.

**Syntax** `show running-config firewall`

**Mode** Privileged Exec

**Examples** To show the configuration commands that have been used to configure the firewall, use the command:

```
awplus# show running-config firewall
```

**Output** Figure 55-13: Example output from the **show running-config firewall** command

```
awplus#show running-config firewall
firewall
 rule 10 permit ping from public to private
 protect
!
```

# 56

# Application and Entity Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure application and entity. For more information, see the [Firewall\\_and Network Address Translation \(NAT\) Feature Overview and Configuration\\_Guide](#).

The table below lists the application commands and their applicable modes.

Figure 56-1: Application commands and applicable modes

| Mode                 | Command                              |
|----------------------|--------------------------------------|
| Privileged Exec      | <code>show application</code>        |
|                      | <code>show application detail</code> |
| Global Configuration | <code>application</code>             |
| Application Mode     | <code>protocol</code>                |
|                      | <code>icmp-type</code>               |
|                      | <code>icmp-code</code>               |
|                      | <code>sport</code>                   |
|                      | <code>dport</code>                   |

The table below lists the entity commands and their applicable modes.

Figure 56-2: Entity commands

| Mode                 | Command                     |
|----------------------|-----------------------------|
| Privileged Exec      | <code>show entity</code>    |
| Global Configuration | <code>zone</code>           |
| Zone Mode            | <code>network (zone)</code> |

| Mode         | Command                          |
|--------------|----------------------------------|
| Network Mode | <code>ip subnet</code>           |
|              | <code>ipv6 subnet</code>         |
|              | <code>host (network)</code>      |
| Host Mode    | <code>ip address (host)</code>   |
|              | <code>ipv6 address (host)</code> |

- Command List**
- [“application”](#) on page 2555
  - [“dport”](#) on page 2557
  - [“dscp”](#) on page 2559
  - [“host \(network\)”](#) on page 2561
  - [“icmp-code”](#) on page 2563
  - [“icmp-type”](#) on page 2565
  - [“ip address \(host\)”](#) on page 2567
  - [“ip subnet”](#) on page 2569
  - [“ipv6 address \(host\)”](#) on page 2571
  - [“ipv6 subnet”](#) on page 2573
  - [“mac-address \(host\)”](#) on page 2575
  - [“network \(zone\)”](#) on page 2577
  - [“protocol”](#) on page 2579
  - [“show application”](#) on page 2580
  - [“show application detail”](#) on page 2581
  - [“show entity”](#) on page 2584
  - [“sport”](#) on page 2587
  - [“zone”](#) on page 2589

# application

**Overview** Use this command to create or modify a custom application.

An application is a high level abstraction of application packets being transported by network traffic. Traffic matching for applications can be achieved by using several techniques, for example, matching packets to port numbers or searching for application signatures in flows of packets.

You can use the tab key to auto-complete application names.

Use the **no** variant of this command to delete a custom application.

**Syntax** `application <application-name>`  
`no application <application-name>`

| Parameter                             | Description                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;application-name&gt;</code> | Application name.<br>You can use all alphanumeric ASCII characters, and the dash (-) and underscore (_) characters. The name can be 1 to 64 characters long. The application name is case-sensitive. If you create two application names with the same spelling but one in upper case and the other one in lower case, the last overwrites the first entry. |

**Mode** Global Configuration

**Usage notes** Use this command to enter the Application Configuration mode, to create a custom application or configure an existing application. You can configure the source port, destination port, protocol, ICMP code and ICMP type for the application. An application is invalid if its protocol, source or destination are not properly configured, for example, if the application has no protocol configured, or source and destination ports are applied to protocols that are not TCP, UDP or SCTP.

There are 40 predefined applications with protocols, source and destinations ports.

You can change the protocol, source and destination ports of the predefined applications. You can only delete the predefined application when you change either its protocol, source or destination port.

Use the [show application](#) command to show all the custom and predefined applications.

**Examples** To create a custom application named 'isakmp', use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)#
```

To delete the custom application named 'isakmp', use the commands:

```
awplus# configure terminal
awplus(config)# no application isakmp
```

**Related  
commands**

dport  
icmp-code  
icmp-type  
protocol  
show application  
sport



# dport

**Overview** Use this command to specify a destination port or port range for an application.

A port number is part of the addressing information used to identify a specific process to which a network message is to be forwarded between a sender and a receiver. For the full list of port numbers and their assignment, you can visit the Internet Assigned Numbers Authority (IANA) website at [www.iana.org](http://www.iana.org).

Use the **no** variant of this command to delete a port or a port range from an application. Note that the port or port range that you want to delete must match exactly the existing port or port range. You cannot remove a port range that is part of an existing port range.

**Syntax** `dport {<destination-port>|any|<start-range> to <end-range>}`  
`no dport {<destination-port>|any|<start-range> to <end-range>}`

| Parameter                             | Description                                                                                     |
|---------------------------------------|-------------------------------------------------------------------------------------------------|
| <code>&lt;destination-port&gt;</code> | The destination port number, either TCP or UDP, specified as an integer in the range <1-65535>. |
| <code>any</code>                      | Any port number in the range <1-65535>. This equals to a range of 1 to 65535.                   |
| <code>&lt;start-range&gt;</code>      | Starting port number in the range <1-65535>.                                                    |
| <code>to &lt;end-range&gt;</code>     | Ending port number in the range <1-65535> or <b>max</b> .                                       |

**Mode** Application Mode

**Usage notes** You can have up to 15 **dports** per application. This is counted as follows:

- a single **dport** counts as 1 port
- a range counts as 2 ports
- the keyword **any** counts as 2 ports.

**Examples** To specify destination port 500 for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# dport 500
```

To specify destination port 500 and a range of ports for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# dport 500
awplus(config-application)# dport 60000 to max
```

To specify the destination port any (a port number range of 1-65535) for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# dport any
```

To remove destination port 500 from the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# no dport 500
```

To remove port **any** from the application isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# no dport 1 to 65535
```

**Related  
commands**

[application](#)  
[sport](#)  
[show application](#)

# dscp

**Overview** Use this command to specify one or more DSCP values used by an application.

Use the **no** variant of this command to remove one or more DSCP values from an application.

**Syntax**

```
dscp <dscp-list>
```

```
dscp {af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|ef|be}
```

```
dscp {cs0|cs1|cs2|cs3|cs4|cs5|cs6|cs7}
```

```
no dscp
```

```
no dscp <dscp-list>
```

```
no dscp {af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|ef|be}
```

```
no dscp {cs0|cs1|cs2|cs3|cs4|cs5|cs6|cs7}
```

| Parameter   | Description                                                                                                                                                                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <dscp-list> | One or more DSCP values, in the range 0-63. Use spaces to separate values.                                                                                                                                                                                                       |
| af11 ... be | One or more DSCP values specified according to the Assured Forwarding group, as defined in RFC 2597 and RFC 3260. See the table below for values. "ef" means expedited forwarding (DSCP 46) and "be" means best effort (DSCP 0). Voice traffic is typically given a value of ef. |
| cs0 ... cs7 | One or more DSCP values specified according to the Class Selector group. This is equivalent to TOS IP precedence values, so that CS0 is equivalent to an IP precedence value of 0, CS1 is equivalent to an IP precedence value of 1, and so on.                                  |

Table 56-1: Assured Forwarding (AF) behavior group

|                         | Class 1           | Class 2           | Class 3           | Class 4           |
|-------------------------|-------------------|-------------------|-------------------|-------------------|
| Low drop probability    | AF11<br>(DSCP 10) | AF21<br>(DSCP 18) | AF31<br>(DSCP 26) | AF41<br>(DSCP 34) |
| Medium drop probability | AF12<br>(DSCP 12) | AF22<br>(DSCP 20) | AF32<br>(DSCP 28) | AF42<br>(DSCP 36) |
| High drop probability   | AF13<br>(DSCP 14) | AF23<br>(DSCP 22) | AF33<br>(DSCP 30) | AF43<br>(DSCP 38) |

**Mode** Application Mode

**Usage notes** You can specify only one set of DSCP values for an application. The newly specified list will replace the existing one; it will not be added to the existing one.

**Example** To specify a DSCP of **ef** for the application named **voice**, use the commands:

```
awplus# configure terminal
awplus(config)# application voice
awplus(config-application)# dscp ef
```

To specify DSCPs of 12 and 13 for the application named **test**, use the commands:

```
awplus# configure terminal
awplus(config)# application test
awplus(config-application)# dscp 12 13
```

To remove DSCP12 from the application named **test**, use the commands:

```
awplus# configure terminal
awplus(config)# application test
awplus(config-application)# no dscp 12
```

To stop the application named **test** from using DSCP values, use the commands:

```
awplus# configure terminal
awplus(config)# application test
awplus(config-application)# no dscp
```

**Related commands**

- [application](#)
- [show application](#)
- [show application detail](#)

# host (network)

**Overview** Use this command to add a host to a network entity or to configure an existing host.

Host is a high level abstraction of a single node in a network. This is commonly used if a particular device, for example a server, has a static IP address that needs to be specified in a firewall policy.

Use the **no** variant of this command to remove a host from a network entity.

**Syntax** `host <host-name>`  
`no host <host-name>`

| Parameter                      | Description                                                                                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;host-name&gt;</code> | Host name.<br>You can use all alphanumeric ASCII characters, and the dash (-) and underscore (_) characters. The name can be 1 to 64 characters in long. |

**Mode** Network Mode

**Usage notes** You can create multiple hosts for a network. A host entity is identified by its parent network using the dot notation, for example, ZoneName.NetworkName.HostName.

This commands allows you to enter the Host Mode with the prompt **awplus(config-host)#**. The Host Mode enables you to configure IPv4 address and IPv6 address for the host. For more information about host IPv4 address and IPv6 address, see [ip address \(host\)](#) command and [ipv6 address \(host\)](#) command respectively.

**Example** To create a host entity named `ftp` under network entity `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# host ftp
awplus(config-host)#
```

To remove host entity `ftp` and its IP address configuration from network entity `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# no host ftp
```

**Related  
commands**

[ip address \(host\)](#)  
[ipv6 address \(host\)](#)  
[mac-address \(host\)](#)  
[network \(zone\)](#)  
[show entity](#)

# icmp-code

**Overview** Use this command to configure an ICMP message code for an application.

ICMP has many messages that are identified by a “type” field and many of these ICMP types have a “code” field. Use the [icmp-type](#) command to specify the ICMP type. For the full list of the ICMP code assignments, you can visit the Internet Assigned Numbers Authority (IANA) website at [www.iana.org](http://www.iana.org).

Use the **no** variant of this command to restore the ICMP message code to its default, which is **any**.

**Syntax** `icmp-code {<code-number>|any}`  
`no icmp-code`

| Parameter                        | Description                                                   |
|----------------------------------|---------------------------------------------------------------|
| <code>&lt;code-number&gt;</code> | Specify an ICMP message code number in the range of 0 to 255. |
| <code>any</code>                 | Any ICMP message code in the range of 0 to 255.               |

**Default** The default ICMP code number is **any**.

**Mode** Application Mode

**Usage notes** You should configure the ICMP code only for applications that use protocol ICMP. To configure the application protocol, see the [protocol](#) command.

You can specify only one ICMP message code for an application. The newly specified code will replace the previous one.

**Examples** To specify ICMP code 5 (redirect) for the application named icmp, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# icmp-code 5
```

To specify the ICMP code as **any** for the application named icmp, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# icmp-code any
```

To restore the ICMP message code to its default of **any** for the application named icmp, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# no icmp-code
```

**Related  
commands**

- application
- icmp-type
- protocol
- show application



# icmp-type

**Overview** Use this command to configure an ICMP message type for an application.

The ICMP protocol has many messages that are identified by a “type” field. For the full list of the ICMP type assignments, you can visit the Internet Assigned Numbers Authority (IANA) website at [www.iana.org](http://www.iana.org).

Use the **no** variant of this command to restore the ICMP message type to its default, which is **any**.

**Syntax** icmp-type {<type-number>|any}  
no icmp-type

| Parameter     | Description                                                   |
|---------------|---------------------------------------------------------------|
| <type-number> | Specify an ICMP message type number in the range of 0 to 255. |
| any           | Any ICMP message type in the range of 0 to 255.               |

**Default** The default ICMP type is **any**.

**Mode** Application Mode

**Usage notes** You should configure the ICMP type only for applications that use protocol ICMP. To configure the application protocol, see the [protocol](#) command.

You can specify only one ICMP message type for an application. The newly specified type will replace the previous one.

**Examples** To specify ICMP message type 8 (echo) for the application named icmp, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# icmp-type 8
```

To specify the ICMP message type as **any** for the application named icmp, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# icmp-type any
```

To restore the ICMP message type to its default of **any** for the application named icmp, use the commands:

```
awplus# configure terminal
awplus(config)# application icmp
awplus(config-application)# no icmp-type
```

**Related  
commands**

- application
- icmp-code
- network (zone)
- show application

# ip address (host)

**Overview** Use this command to assign an IPv4 address to a host entity.  
Use the **no** variant of this command to remove an IPv4 address from the host.

**Syntax**

```
ip address <ipv4-address>
ip address dynamic fqdn <domain_name>
ip address dynamic interface <interface_name>
no ip address <ipv4-address>
no ip address dynamic fqdn <domain_name>
no ip address dynamic interface <interface_name>
```

| Parameter        | Description                                                   |
|------------------|---------------------------------------------------------------|
| <ipv4-address>   | The IPv4 address uses the format A.B.C.D.                     |
| dynamic          | Dynamic IP address, for example, obtained from a DHCP server. |
| <domain_name>    | The FQDN to resolve IP addresses for.                         |
| <interface_name> | Interface to acquire IP addresses from.                       |

**Mode** Host

**Usage notes** You can add multiple IP addresses to a host entity. If the IP address is not in the scope of any of its parent network's IPv4 subnets, a warning message will be given. Such an IP address is still acceptable because in the future the user may assign a network subnet that contains the host's IP address. Firewall policy rules will not apply to an IP address that is not in at least one of the network's subnets.

If you are adding an FQDN, DNS Relay cache and **ip domain-lookup via-relay** must be enabled for this command to work. DNS requests passing through the router are inspected for matching FQDNs. Because of this, the DNS cache is cleared when this command is entered so that the IP addresses can be picked up.

You can add multiple dynamic FQDNs for a host entity.

Domain names will match the most specific FQDN entity available, with subdomains matching less specific FQDNs when necessary.

This functions similarly to a wildcard DNS record. For example, with the FQDN entities 'com,' 'google.com,' and 'maps.google.com' configured, 'microsoft.com' will match 'com,' 'drive.google.com' will match 'google.com,' and 'maps.google.com' will match 'maps.google.com' rather than 'google.com'.

**Examples** To add an IP address to host ftp, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 192.168.1.0/24
awplus(config-network)# host ftp
awplus(config-host)# ip address 192.168.1.5
```

To add multiple IP addresses to host ftp, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 192.168.1.0/24
awplus(config-network)# host ftp
awplus(config-host)# ip address 192.168.1.8
awplus(config-host)# ip address 192.168.1.9
awplus(config-host)# ip address 192.168.1.10
```

To add the IPv4 addresses of the FQDN "google.com" to a zone, use the following commands:

```
awplus# configure terminal
awplus(config)# zone Public
awplus(config-zone)# network Router
awplus(config-network)# ip subnet 0.0.0.0/0
awplus(config-network)# host google
awplus(config-host)# ip address dynamic fqdn google.com
```

To remove an IP address from host ftp, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# host ftp
awplus(config-host)# no ip address 192.168.1.5
```

**Validation  
commands** [show entity](#)

**Related  
commands** [host \(network\)](#)  
[ip domain-lookup](#)

**Command  
changes** Version 5.4.8-1.1: FQDN parameter and output added

# ip subnet

**Overview** Use this command to add an IPv4 subnet to a network entity.

Use the **no** variant of this command to remove a subnet from a network entity.

**Syntax** `ip subnet <ip-network/m> [interface <interface-name>]`  
`no ip subnet <ip-network/m> [interface <interface-name>]`

| Parameter        | Description                                                                                                                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-network/m>   | IP address of the network, entered in the form A.B.C.D/M. Dotted decimal notation followed by a forward slash, and then the subnet mask length.                                                                  |
| interface        | Specify an interface name. An interface may be specified to add a further restriction on the subnet. No interface configured indicates that any matching address from any interface is a member of this network. |
| <interface-name> | Interface name. Any AlliedWare Plus interface type (eth, ppp, tunnel, lo, etc.) followed by any character.<br>A warning message is given if the interface does not match an existing interface on the device.    |

**Mode** Network Mode

**Usage notes** You can create multiple subnets to a network entity.

**Examples** To add a subnet to network 'servers', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 192.168.2.0/24
```

To add a subnet and an interface to network 'servers', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 192.168.2.0/24 interface eth1
```

To add multiple subnets to network 'servers', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ip subnet 192.168.2.0/24 interface eth1
awplus(config-network)# ip subnet 10.1.0.0/16 interface eth1
```

To remove a subnet from network 'servers', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# no ip subnet 192.168.2.0/24
```

**Related  
commands**   [network \(zone\)](#)  
[show entity](#)

# ipv6 address (host)

**Overview** Use this command to assign an IPv6 address to a host entity.

Use the **no** variant of this command to remove an IPv6 address from an host entity.

**Syntax**

```
ipv6 address <ipv6-address>
ipv6 address dynamic fqdn <domain_name>
ipv6 address dynamic interface <interface_name>
no ipv6 address <ipv6-address>
no ipv6 address dynamic fqdn <domain_name>
no ipv6 address dynamic interface <interface_name>
```

| Parameter        | Description                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv6-address>   | The IPv6 address in the format x:x::x:x.                                                                                                                        |
| dynamic          | Dynamic IPv6 address, for example, obtained from a DHCP server.                                                                                                 |
| <domain_name>    | The FQDN to resolve IP addresses for. Valid characters are any printable character. If the name contains spaces, then you must enclose it in "quotation marks". |
| <interface_name> | Interface to acquire IP addresses from.                                                                                                                         |

**Mode** Host

**Usage notes** You can add multiple IPv6 addresses to a host entity. If the IPv6 address is not in the scope of any of its parent network's IPv6 subnets, a warning message will be given. Such an IP address is still acceptable because in the future the user may assign a network subnet that contains the host's IPv6 address. Firewall policy rules will not apply to an IPv6 address that is not in at least one of the network's subnets.

If you are adding an FQDN, DNS Relay cache and **ip domain-lookup via-relay** must be enabled for this command to work. DNS requests passing through the router are inspected for matching FQDNs. Because of this, the DNS cache is cleared when this command is entered so that the IPv6 addresses can be picked up.

You can add multiple dynamic FQDNs for a host entity.

Domain names will match the most specific FQDN entity available, with subdomains matching less specific FQDNs when necessary.

This functions similarly to a wildcard DNS record. For example, with the FQDN entities 'com,' 'google.com,' and 'maps.google.com' configured, 'microsoft.com' will match 'com,' 'drive.google.com' will match 'google.com,' and 'maps.google.com' will match 'maps.google.com' rather than 'google.com'.

**Examples** To add an IPv6 address to the host named 'web-server', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ipv6 subnet 2001:db8:24:100::/64
awplus(config-network)# host web-server
awplus(config-host)# ipv6 address 2001:db8:24:100::1
```

To add multiple IP addresses to the host named 'web-server', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ipv6 subnet 2001:db8:24:100::/64
awplus(config-network)# host web-server
awplus(config-host)# ipv6 address 2001:db8:24:100::2
awplus(config-host)# ipv6 address 2001:db8:24:100::3
awplus(config-host)# ipv6 address 2001:db8:24:100::4
```

To add the IPv6 addresses of the FQDN 'google.com' to a zone, use the following commands:

```
awplus# configure terminal
awplus(config)# zone Public
awplus(config-zone)# network Router
awplus(config-network)# ip subnet ::/0
awplus(config-network)# host google
awplus(config-host)# ip address dynamic fqdn google.com
```

To remove an IPv6 address from the host named 'web-server', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# host web-server
awplus(config-host)# no ipv6 address 2001:db8:24:100::2
```

**Validation  
commands** [show entity](#)

**Related  
commands** [host \(network\)](#)  
[ip domain-lookup](#)

**Command  
changes** Version 5.4.8-1.1: FQDN parameter and output added



# ipv6 subnet

**Overview** Use this command to assign an IPv6 subnet to a network entity.  
Use the **no** variant of this command to remove a IPv6 subnet from a network entity.

**Syntax** `ipv6 subnet <ip-network/m> [interface <interface-name>]`  
`no ipv6 subnet <ip-network/m> [interface <interface-name>]`

| Parameter        | Description                                                                                                                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-network/m>   | IPv6 address of the network, entered in the form X:X::X/M, followed by the prefix length in slash notation.                                                                                                      |
| interface        | Specify an interface name. An interface may be specified to add a further restriction on the subnet. No interface configured indicates that any matching address from any interface is a member of this network. |
| <interface-name> | Interface name. Any AlliedWare Plus interface type (eth, ppp, tunnel, lo, etc.) followed by any character.<br>A warning message is given if the interface does not match an existing interface on the device.    |

**Mode** Network Mode

**Usage notes** You can create multiple subnets for a network entity.

**Examples** To add a subnet to network 'servers', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ipv6 subnet 2001:db8::/32
```

To add a subnet and an interface to network 'servers', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ipv6 subnet 2001:db8::/32 interface
eth1
```

To add multiple subnets to network 'servers', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# ipv6 subnet 2001:db8::7/32 interface
eth1
awplus(config-network)# ipv6 subnet 2001:db8::8/32 interface
eth1
```

To remove a subnet from network 'servers', use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)# no ipv6 subnet 2001:db8::/32
```

**Related  
commands**   [network \(zone\)](#)  
[show entity](#)

## mac-address (host)

**Overview** Use this command to filter packets that come from particular hosts. You do this by attaching the host's MAC address to the host entity.

This is a useful alternative to filtering by IP address, especially if the host's IP address is allocated dynamically.

You can use this filtering, for example, to increase security by preventing internal sensors from sending information out to the Internet.

You can add multiple MAC addresses for a given host entity, if more than one device is part of the entity.

Use the **no** variant of this command to remove a MAC address from the host.

**Syntax** `mac-address <mac-address>`  
`no mac-address <mac-address>`

| Parameter                        | Description                                                       |
|----------------------------------|-------------------------------------------------------------------|
| <code>&lt;mac-address&gt;</code> | A MAC address to match on, specified in XX:XX:XX:XX:XX:XX format. |

**Default** No MAC addresses are attached to host entities

**Mode** Host

**Usage notes** This feature matches on incoming packets. This means you should use it with Firewall or NAT rules where the entity is in the **from** field.

MAC addresses specified with this command are not used for matching in Web Control or DPI Detailed Counters.

**Example** To add the MAC address 00:00:cd:11:22:33 to the entity named example.cameras.door, use the commands:

```
awplus# configure terminal
awplus(config)# zone example
awplus(config-zone)# network cameras
awplus(config-network)# host door
awplus(config-host)# mac-address 00:00:cd:11:22:33
```

To use this example.cameras.door entity to block traffic from the camera to the Internet, use the commands:

```
awplus# configure terminal
awplus(config)# firewall
awplus(config-firewall)# rule deny any from
example.cameras.door to inet
awplus(config-firewall)# protect
```

To remove the MAC address 00:00:cd:11:22:33 from the entity, use the commands:

```
awplus# configure terminal
awplus(config)# zone example
awplus(config-zone)# network cameras
awplus(config-network)# host door
awplus(config-host)# no mac-address 00:00:cd:11:22:33
```

**Related  
commands**

- [host \(network\)](#)
- [network \(zone\)](#)
- [show entity](#)
- [zone](#)

**Command  
changes**

- Version 5.5.3-1.1: command added

# network (zone)

**Overview** Use this command to add a network to a zone entity or configure an existing network.

A network is a high level abstraction of a logical network in a zone. This consists of the IP subnets and interfaces over which it is reachable. Subnets are grouped into networks to apply a common set of rules among the subnets.

Use the **no** variant of this command to destroy a network entity.

**Syntax** `network <network-name>`  
`no network <network-name>`

| Parameter                         | Description                                                                                                                                                 |
|-----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;network-name&gt;</code> | Network name.<br>You can use all alphanumeric ASCII characters, and the dash (-) and underscore (_) characters. The name can be 1 to 64 characters in long. |

**Mode** Zone Mode

**Usage notes** A network is a member of a zone. You can create multiple networks in a zone. A network entity is identified with its parent zone using the dot notation, for example, ZoneName.NetworkName.

This commands allows you to enter the Network Mode with the prompt **awplus(config- network)#**. In the Network Mode, you can:

- Configure subnets and interfaces for the network entity
- Create and delete host entities in the network

A network must have at least one valid network address for it to result in functioning rules using that network entity. For more information about how to add network address, see the [ip subnet](#) command and the [ipv6 subnet](#) command.

Note that if the network entity is destroyed, the subnets and hosts in the network entity will be destroyed as well.

**Example** To create a network entity named `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# network servers
awplus(config-network)#
```

To destroy a network entity named `servers`, use the commands:

```
awplus# configure terminal
awplus(config)# zone dmz
awplus(config-zone)# no network servers
```

**Validation  
commands**    `show entity`

**Related  
commands**    `host (network)`  
              `ip subnet`  
              `ipv6 subnet`  
              `zone`

# protocol

**Overview** Use this command to specify a protocol used by an application.

Protocol numbers are used to configure firewalls, routers, and proxy servers. The protocol number is in the protocol field of the IPv4 header and the next header field of IPv6 header. For the full list of the IP Protocol assignments, you can visit the Internet Assigned Numbers Authority (IANA) website at [www.iana.org](http://www.iana.org).

Use the **no** variant of this command to unset the protocol in an application.

**Syntax** `protocol {tcp|udp|icmp|ipv6-icmp|<protocol-number>}`  
`no protocol`

| Parameter         | Description                                                                                   |
|-------------------|-----------------------------------------------------------------------------------------------|
| tcp               | Transmission Control Protocol. The protocol number is 6.                                      |
| udp               | User Datagram Protocol. The protocol number is 17.                                            |
| icmp              | Internet Control Message Protocol for Internet Protocol version 4. The protocol number is 1.  |
| ipv6-icmp         | Internet Control Message Protocol for Internet Protocol version 6. The protocol number is 58. |
| <protocol-number> | Protocol number in the range of 0 to 255.                                                     |

**Mode** Application Mode

**Usage notes** You can specify only one protocol for an application. The newly specified protocol will replace the previous one.

**Examples** To specify protocol udp for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# protocol udp
```

To unset the protocol in the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# no protocol
```

**Related commands** [application](#)  
[show application](#)

# show application

**Overview** Use this command to show the custom and predefined applications currently configured.

You can use the [show application detail](#) command to show detailed information of the applications.

**Syntax** `show application`

**Mode** Privileged Exec

**Examples** To show all applications currently configured, use the command:

```
awplus# show application
```

**Output** Figure 56-3: Example output from **show application**

```
awplus#show application
aim cvs dns ftp
http https icq ident
imap imaps irc jabber
l2tp ldap lisa msn
mysql news nfs-tcp nfs-udp
ntp openvpn pcanywhere udp
...
```

**Related commands** [show application detail](#)



# show application detail

**Overview** Use this command to show detailed information about applications that the device is aware of. For custom and predefined applications, the protocol, destination port, source port, ICMP code, ICMP type, DSCP and the name of the applications will be displayed.

For applications defined by DPI, a description of the application is displayed.

**Syntax** `show application detail [<name>|custom|dpi]`

| Parameter | Description                                                                                                                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <name>    | The name of a specific application.                                                                                                                                                                 |
| custom    | User-defined application.                                                                                                                                                                           |
| dpi       | DPI applications. For DPI applications to be displayed by this command, you must first enable DPI by using the <a href="#">enable (dpi)</a> command and the <a href="#">provider (dpi)</a> command. |

**Mode** Privileged Exec

**Examples** To show the information about all applications, use the command:

```
awplus# show application detail
```

**Output** To show the information about the application ping, use the command:

```
awplus# show application detail ping
```

Figure 56-4: Example output from **show application detail** for an application

```
awplus#show application detail ping
Name Mark Detail

ping - proto=ICMP type=8 code=0
```

Figure 56-5: Example output from **show application detail** with provider **built-in**

```
area3[1]#show application detail
```

| Name        | Mark | Detail                                                                                                             |
|-------------|------|--------------------------------------------------------------------------------------------------------------------|
| afp         | 0x6A | DPI: Apple Filing Protocol, formerly AppleTalk<br>(Cat=File transfer)                                              |
| aim         | -    | proto=TCP sport=1024-65535 dport=9898                                                                              |
| aimini      | 0x6C | DPI: Aimini P2P real-time communicatings<br>(Cat=Messaging)                                                        |
| ajp         | 0x94 | DPI: Apache JServ Protocol (Cat=Networking)                                                                        |
| amazon      | 0xBB | DPI: Amazon online shopping (Cat=Web Services)                                                                     |
| amazonvideo | 0xF9 | DPI: Amazon on-demand video streaming service<br>(Cat=Streaming Media)                                             |
| amqp        | 0xC9 | DPI: Advanced Message Queuing Protocol<br>(Cat=Networking)                                                         |
| apple       | 0x95 | DPI: Apple Inc website (Cat=Networking)                                                                            |
| appleicloud | 0x98 | DPI: A cloud storage and cloud computing service from<br>Apple Inc (Cat=File transfer)                             |
| appleitunes | 0x9A | DPI: A media streaming, broadcasting, and device<br>management application from Apple Inc<br>(Cat=Streaming Media) |
| applejuice  | 0x21 | DPI: A defunct file sharing protocol (Cat=File<br>transfer)                                                        |
| ...         |      |                                                                                                                    |

Figure 56-6: Example output from **show application detail** with provider **procera**

```
awplus#show application detail
```

| Name     | Mark  | Detail                                                                                                                                 |
|----------|-------|----------------------------------------------------------------------------------------------------------------------------------------|
| 050plus  | 0x435 | DPI: The traffic consists of data from<br>logging in or making calls with the 050Plus<br>application. (Cat=Messaging, Prod=2, Risk=2)  |
| 12306cn  | 0x292 | DPI: 12306.cn is the only China Railway<br>customer service center (Cat=Web Services,<br>Prod=4, Risk=1)                               |
| 123movie | 0x64D | DPI: Free movie streaming/downloading site<br>(Cat=Streaming Media, Prod=1, Risk=5)                                                    |
| 126com   | 0x293 | DPI: 126.com is a free webmail service of<br>Netease (Cat=Mail, Prod=4, Risk=2)                                                        |
| 17173    | 0x30B | DPI: General browsing, interaction, and game<br>play on the social gaming network 17173.com<br>(Cat=Social Networking, Prod=2, Risk=2) |
| 1fichier | 0x779 | DPI: Online cloud storage. (Cat=File Transfer,<br>Prod=1, Risk=5)                                                                      |
| ...      |       |                                                                                                                                        |

Table 56-2: Parameters in the output from **show application detail**

| Parameter | Description                                                                                                                                                                                                                                                                                                                       |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name      | Application name—the short name used when referenced from application-aware features (for instance firewall).                                                                                                                                                                                                                     |
| Mark      | Application mark—the hexadecimal DPI application index representing each protocol or application. This value appears in Firewall log messages, indicating which application the packet or flow was identified as by DPI.                                                                                                          |
| Detail    | For custom and pre-defined applications—the IP protocol and port numbers associated with the application. For DPI applications— a longer description of the application.                                                                                                                                                          |
| Cat       | Category—a general and high-level category for the application.                                                                                                                                                                                                                                                                   |
| Prod      | Productivity—an index value between 1 and 5 that rates the potential for each application to improve or increase the overall productivity of network users. For instance, applications with a low productivity index (e.g. games and social networking) can be expected to have a negative impact on productivity. (Procera only) |
| Risk      | Risks—an index value between 1 and 5 that rates the potential for each protocol or application to allow undesirable content onto your network. The higher the risk index, the greater the chance of letting in something that could be dangerous or destructive. (Procera only)                                                   |

**Related commands** [show application](#)

**Command changes** Version 5.4.7-2.1: More detail added to the output for DPI commands.  
Version 5.4.9-1.1: Category added to output for built-in provider

# show entity

**Overview** Use this command to show entity information.

Entity is a high level abstraction of a network device, a group of networks or subnets. It is the instance that firewall policy can be applied to. There are three types of entity:

- zone
- network
- host

**Syntax** `show entity [<entity>]`

| Parameter | Description                      |
|-----------|----------------------------------|
| <entity>  | Specific entity in dot notation. |

**Mode** Privileged Exec

**Examples** To show the information about all entities, use the command:

```
awplus# show entity
```

**Output** Figure 56-7: Example output from the **show entity** command

```
awplus#show entity
Zone: zone1
Network: zone1.network1
Subnet: 1:db8:24:100::/64
Subnet: 2001:db8:24:100::/64
Host: zone1.network1.host1
Address: 2001:db8:24:100::1

Zone: zone2
Network: zone2.network2
Host: zone2.network2.host1
```

To show information associated with the network entity `zone1.network1`, use the command:

```
awplus# show entity zone1.network1
```

**Output** Figure 56-8: Example output from the **show entity** command

```
awplus#show entity zone1.network1
Network: zone1.network1
Subnet: 1:db8:24:100::/64
Subnet: 2001:db8:24:100::/64
Host: zone1.network1.host1
Address: 2001:db8:24:100::1
```

To show information associated with the host entity `zone1.network1.host1`, use the command:

```
awplus# show entity zone1.network1.host1
```

**Output** Figure 56-9: Example output from the **show entity** command

```
awplus#show entity zone1.network1.host1
Host: zone1.network1.host1
Address: 192.168.1.5
```

When the entity is using dynamic interface addresses, this will be shown in the output:

**Output** Figure 56-10: Example output from the **show entity** command

```
awplus#show entity Public
Zone: Public
Network: Public.Router
Subnet: 0.0.0.0/0 via ppp0
Host: Public.Router.ppp0
Address: 10.0.6.1 (dynamic)
```

When the entity is using dynamic FQDN addresses, this will be shown in the output:

**Output** Figure 56-11: Example output from the **show entity** command using dynamic FQDN addresses on the console

```
awplus#show entity Public
Zone: Public
Network: Public.FQDNs
Subnet: 0.0.0.0/0
Subnet: ::/0
Host: Public.FQDNs.alliedtelesis
FQDN IPv4: alliedtelesis.com
FQDN IPv6: alliedtelesis.com
Address: 54.66.120.42 (dynamic)
```

```
Host: Public.FQDNs.facebook
FQDN IPv4: facebook.com
FQDN IPv6: facebook.com
Address: 157.240.8.35 (dynamic)
Address: 2a03:2880:f119:8083:face:b00c:0:25de (dynamic)
Host: Public.FQDNs.google
FQDN IPv4: google.com
FQDN IPv6: google.com
Address: 216.58.196.142 (dynamic)
Address: 2404:6800:4006:809::200e (dynamic)
Host: Public.FQDNs.microsoft
FQDN IPv4: microsoft.com
FQDN IPv6: microsoft.com
Address: 23.96.52.53 (dynamic)
Address: 23.100.122.175 (dynamic)
Address: 104.40.211.35 (dynamic)
Address: 104.43.195.251 (dynamic)
Address: 191.239.213.197 (dynamic)
```

**Command  
changes**

Version 5.4.8-1.1: added output for dynamic interface and FQDN addresses.

# sport

**Overview** Use this command to specify a source port or a port range used for an application.

A port number is part of the addressing information used to identify a specific process to which a network message is to be forwarded between a sender and a receiver. For the full list of port numbers and their assignment, you can visit the Internet Assigned Numbers Authority (IANA) Web site: [www.iana.org](http://www.iana.org).

Use the **no** variant of this command to delete ports or port ranges from an application.

**NOTE:**

The port or port range that you want to delete must match exactly the existing port or port range. You cannot remove a port range that is part of an existing port range.

**Syntax** `sport {<source-port>|any|<start-range> to <end-range>}`  
`no sport {<source-port>|any|<start-range> to <end-range>}`

| Parameter         | Description                                                                             |
|-------------------|-----------------------------------------------------------------------------------------|
| <source-port>     | The source port number, either TCP or UDP, specified as an integer between 1 and 65535. |
| any               | Any port number in the range <1-65535>. This equals to a range of 1 to 65535.           |
| <start-range>     | Starting port number in the range <1-65535>.                                            |
| to<br><end-range> | Ending port number in the range <1-65535> or max.                                       |

**Mode** Application Mode

**Usage notes** You can have up to 15 **sports** per application. This is counted as follows:

- a single **sport** counts as 1 port
- a range counts as 2 ports
- the keyword **any** counts as 2 ports.

**Examples** To specify source port 500 for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# sport 500
```

To specify source port 500 and a range of ports for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# sport 500
awplus(config-application)# sport 60000 to max
```

To specify the source port **any** (a port number range of 1-65535) for the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# sport any
```

To remove source port 500 from the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# no sport 500
```

To remove all source ports from the application named isakmp, use the commands:

```
awplus# configure terminal
awplus(config)# application isakmp
awplus(config-application)# no sport 1 to 65535
```

**Related  
commands**

[application](#)

[dport](#)

[show application](#)



# zone

**Overview** Use this command to create a zone entity or configure an existing zone.

Zone is a high level abstraction for a logical grouping or segmentation of physical networks. This is the highest level of partitioning that firewall policy can be applied to. Zone establishes the security border of your networks. A zone defines a boundary where traffic is subjected to policy restrictions as it crosses to another region of your networks. The minimum zones normally implemented would be a trusted zone for the private network behind the firewall and a untrusted zone for the Internet. Other common zones are a Demilitarized Zone (DMZ) for publicly visible web servers and a Virtual Private Network (VPN) zone for remote access users or tunnels to other networks.

Use the **no** variant of this command to destroy a zone entity.

**Syntax** `zone <zone-name>`  
`no zone <zone-name>`

| Parameter                      | Description                                                                                                                                           |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;zone-name&gt;</code> | Zone name.<br>You can use all alphanumeric ASCII characters, and the dash (-) and underscore (_) characters. The name can be 1 to 64 characters long. |

**Mode** Global Configuration

**Usage notes** This command allows you to enter the Zone Mode with the prompt **awplus(config-category)#**. The Zone Mode enables you to create, configure and delete network entities. For more information about network entity, see the [network \(zone\)](#) command.

A zone entity must have at least one network entity for it to result in functioning rules using that zone entity. For more information about how to add network entities, see the [network \(zone\)](#) command.

Note that if the zone entity is destroyed, the networks and hosts of this zone will be destroyed as well.

**Examples** To create a zone named `private`, use the commands:

```
awplus# configure terminal
awplus(config)# zone private
awplus(config-zone)#
```

To destroy zone `private` and all its networks, subnets and hosts, use the commands:

```
awplus# configure terminal
awplus(config)# no zone private
```

**Validation** [show entity](#)  
**commands**

# 57

# NAT Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure Network Address Translation (NAT). For more information about NAT introduction and configuration example, see the [Firewall\\_and Network Address Translation \(NAT\) Feature Overview and Configuration\\_Guide](#).

The following figure lists the NAT commands and their applicable modes.

Figure 57-1: NAT commands and applicable modes

| Mode                 | Command                                 |
|----------------------|-----------------------------------------|
| Privileged Exec      | <code>show nat</code>                   |
|                      | <code>show nat rule</code>              |
|                      | <code>show nat rule config-check</code> |
|                      | <code>show running-config nat</code>    |
| Global Configuration | <code>nat</code>                        |
| NAT Configuration    | <code>enable (nat)</code>               |
|                      | <code>move rule (nat)</code>            |
|                      | <code>rule (nat)</code>                 |

- Command List**
- “[enable \(nat\)](#)” on page 2593
  - “[ip limited-local-proxy-arp](#)” on page 2594
  - “[local-proxy-arp](#)” on page 2595
  - “[move rule \(nat\)](#)” on page 2596
  - “[nat](#)” on page 2597
  - “[rule \(nat\)](#)” on page 2598

- [“show nat”](#) on page 2602
- [“show nat rule”](#) on page 2603
- [“show nat rule config-check”](#) on page 2605
- [“show running-config nat”](#) on page 2606

# enable (nat)

**Overview** Use this command to enable NAT .

Use the **no** variant of this command to disable NAT without losing existing NAT configuration.

**Syntax** enable  
no enable

**Default** NAT is disabled by default.

**Mode** NAT Configuration

**Examples** To enable NAT, use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# enable
```

To disable NAT, use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# no enable
```

**Validation commands** show nat  
show running-config nat

# ip limited-local-proxy-arp

**Overview** Use this command to enable local proxy ARP, but only for a specified set of IP addresses. This makes the device respond to ARP requests for those IP addresses when the addresses are reachable via the interface you are configuring.

To specify the IP addresses, use the command [local-proxy-arp](#).

Use the **no** variant of this command to disable limited local proxy ARP. This stops your device from intercepting and responding to ARP requests for the specified hosts. This allows the hosts to use MAC address resolution to communicate directly with one another.

**Syntax** `ip limited-local-proxy-arp`  
`no ip limited-local-proxy-arp`

**Default** Limited local proxy ARP is disabled by default.

**Mode** Interface Configuration for Eth, L2TP tunnel, Multipoint VPN GRE, and bridge interfaces and 802.1Q sub-interfaces.

**Usage** Limited local proxy ARP supports Static NAT configurations in which the NAT configuration's public address is different to the Ethernet interface's address. On such Ethernet interfaces, the device needs to respond to ARP requests for the public address so that it will receive packets targeted at that address. Limited local proxy ARP makes this possible. It is especially useful when you have a number of 1-1 NAT configurations and each public address falls within the public interface's subnet. If you enable limited local proxy ARP on the public interface and specify suitable addresses, the device will respond to ARP requests for those addresses, as long as the addresses are routed out the interface the ARP requests are received on. The device responds with its own MAC address.

**Related commands** [ip local-proxy-arp](#)  
[local-proxy-arp](#)

# local-proxy-arp

**Overview** Use this command to specify an IP subnet for use with limited local proxy ARP. When limited local proxy ARP is enabled with the command [ip limited-local-proxy-arp](#), the device will respond to ARP requests for addresses in that subnet.

Use the **no** variant of this command to stop specifying a subnet for use with limited local proxy ARP.

**Syntax** `local-proxy-arp [<ip-add/mask>]`  
`no local-proxy-arp [<ip-add/mask>]`

| Parameter                        | Description                                                                                                                                 |
|----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-add/mask&gt;</code> | The IP subnet to use with limited local proxy ARP, in dotted decimal format (A.B.C.D/M). To specify a single IP address, use a 32-bit mask. |

**Default** No subnets are specified for use with limited local proxy ARP.

**Mode** Global Configuration

**Example** To specify limited local proxy ARP for the address 172.22.0.3, use the following commands:

```
awplus# configure terminal
awplus(config)# local-proxy-arp 172.22.0.3/32
```

This is part of a configuration snippet that shows how to use limited local proxy ARP with static NAT. See the command [ip limited-local-proxy-arp](#) for the whole example.

**Related commands** [ip limited-local-proxy-arp](#)

## move rule (nat)

**Overview** Use this command to change the order of a NAT rule.

You can move an existing rule ID only to an ID that is not assigned to any rule, otherwise you will receive an error message.

**Syntax** `move rule <1-65535> to <1-65535>`

| Parameter                                  | Description                                                                                                                                                                                                                             |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>move rule<br/>&lt;1-65535&gt;</code> | Move the order of a given rule. The rule ID of the given rule must exist.<br>Each rule has an ID which is either designated by the user or automatically generated when the rule is created. The rule ID is an integer from 1 to 65535. |
| <code>to &lt;1-65535&gt;</code>            | New rule ID to assign. The new rule ID must not be used by any existing rule.                                                                                                                                                           |

**Mode** NAT Configuration

**Examples** To change the ID of a rule from 10 to 30, use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# move rule 10 to 30
```

**Validation commands** `show nat rule`  
`show running-config nat`

**Related commands** `rule (nat)`



# nat

**Overview** Use this command to configure NAT.

Use the **no** variant of this command to remove all NAT configuration.

**Syntax** nat  
no nat

**Mode** Global Configuration

**Usage notes** This command allows you to enter the NAT Configuration mode. The command prompt for this mode is **awplus(config-nat)#**.

In the NAT Configuration mode, you can:

- Enable NAT, see the [enable \(nat\)](#) command.
- Create NAT rules or change the order of NAT rules, see the [rule \(nat\)](#) command and the [move rule \(nat\)](#) command.

**Examples** To configure NAT, use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)#
```

To remove all NAT configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no nat
```

**Validation commands** [show nat](#)

# rule (nat)

**Overview** Use this command to create a NAT rule.

Use the **no** variant of this command to remove a specified rule or all rules.

**Syntax**

```
rule [<1-65535>] masq <application-name> from <source-entity>
to <destination-entity> [with src <source-host-entity>]

rule [<1-65535>] portfw <application-name> from <source-entity>
[to <destination-entity>] with dst <destination-host-entity>
[dport <1-65535>]

rule [<1-65535>] netmap <application-name> from
<source-subnet-entity> to <destination-subnet-entity> with
{src|dst} <translated-subnet-entity>

no rule {<1-65535>|all}
```

| Parameter          | Description                                                                                                                                                                                                                                                               |
|--------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <1-65535>          | Rule ID is an integer in the range 1 to 65535. If you do not designate a rule ID, a rule ID will be automatically generated and it will be greater than the current highest rule ID.                                                                                      |
| masq               | The type of NAT rule. NAT with IP Masquerade is a case where all or a range of addresses are mapped to a single address with source port translation to identify the association. This single address masquerades as the public source address for the private addresses. |
| portfw             | The type of NAT rule. Port forwarding allows remote hosts to connect to a specific host or service within a private LAN. This will forward IPv4 packets on to another device, for example, forward HTTP traffic to an internal web server.                                |
| netmap             | The type of NAT rule. Use subnet-based NAT to translate the subnet portion of IP addresses while leaving the host portion unchanged.                                                                                                                                      |
| <application-name> | In all NAT rules, the application name, either one of the predefined applications or an application defined by using the <b>application</b> command.<br>You can use the tab key to auto-complete application names.                                                       |

| Parameter                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;source-entity&gt;</code>             | <p>Source entity name. An entity represents a logical grouping of subnets, hosts or interfaces, created by the <b>zone</b>, <b>network (Entity)</b>, or <b>host (Entity)</b> commands. You can use the tab key to auto-complete entity names.</p> <p>In a <b>masq</b> rule, the source entity defines the private side of the router. You assign private IP addresses (RFC 1918) to hosts on the private side of the router. When those hosts send traffic, the router translates the private addresses to one or more publicly valid addresses before routing the traffic. When the router receives traffic that is destined for those hosts, it translates the public addresses back to the appropriate private addresses.</p> <p>In a <b>portfw</b> rule, the source entity may be an entity outside your private network.</p> |
| <code>&lt;destination-entity&gt;</code>        | <p>The destination entity name. The destination entity defines the pool of public-valid IP addresses. It can be a zone (created by the <b>zone</b> command), network (<b>network (Entity)</b> command) or host (<b>host (Entity)</b> command).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <code>&lt;source-host-entity&gt;</code>        | <p>In a <b>masq</b> rule, the specific source host address that the traffic will masquerade as. The source -host-entity must be a host with one IP address, created by using the <b>host (Entity)</b> command.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <code>&lt;destination-host-entity&gt;</code>   | <p>In a <b>portfw</b> rule, the target entity name of the specific destination host that the traffic will be port-forwarded to. The target entity must be a host with one IP address, created by using the <b>host (Entity)</b> command.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <code>dport &lt;1-65535&gt;</code>             | <p>In a <b>portfw</b> rule, modify the destination port to the specified port. (Only for protocols that have ports.)</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <code>&lt;source-subnet-entity&gt;</code>      | <p>The source entity that the netmap rule will apply to, for instance a network created by the <b>network (Entity)</b> command. When the <b>with src</b> parameter is used, this source-subnet-entity is translated to the <code>&lt;translated-subnet-entity&gt;</code> specified.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <code>&lt;destination-subnet-entity&gt;</code> | <p>The destination entity that the <b>netmap</b> rule applies to, for instance a network created by the <b>network (Entity)</b> command. When the <b>with dst</b> parameter is used, this destination subnet is translated to the <code>&lt;translated-subnet-entity&gt;</code> specified.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Parameter                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;translated-subnet-entity&gt;</code> | In a <b>netmap</b> rule:<br><b>with src:</b> Modify the source-subnet-entity to the specified translated-subnet-entity, for instance a network created by the <b>network (Entity)</b> command. Both network entities must contain one subnet with a matching subnet mask.<br><b>with dst:</b> Modify the destination-subnet-entity to the specified translated-subnet-entity, for instance a network created by the <b>network (Entity)</b> command. Both network entities must contain one subnet with a matching subnet mask. |
| <code>all</code>                              | Remove all rules.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

**Mode** NAT Configuration

**Usage notes** You can change the rule order by using the [move rule \(nat\)](#) command.

Firewall is used in conjunction with NAT. Port forwarding (**portfw**) and masquerade (**masq**) rules do not implicitly permit packets. **Portfw** rules (actions) are applied before any other firewall and **masq** rules (actions) are applied after any other firewall rules. When firewall protection is enabled, all traffic is blocked by default. Use the [rule \(firewall\)](#) command to configure firewall rules which allow the same application, source and destination entities you configure for the NAT rules.

Netmap **dst** rules are applied to traffic before it reaches the firewall rules, and netmap **src** rules are applied after the firewall has permitted the traffic. Firewall rules must be written to permit the traffic after it has been translated by the netmap **dst** rules.

Entities should have valid interfaces on which inbound and outbound traffic can be properly translated. You can use the [ip subnet](#) command and the [ipv6 subnet](#) command to configure the interfaces.

Removing a NAT rule for an actively translated flow does not stop it translating immediately. This means subsequent packets in the flow continue to be translated.

The continued translation after the associated NAT rule is removed will only stop when:

- The [clear firewall connections](#) command is executed or the flow stops.
- One of the following actions occurs:
  - You can use the [clear firewall connections](#) command to manually stop translations immediately, when the associated rule has been deleted regardless whether the firewall feature is actually configured with NAT or not.
  - The NAT rule is cleared when the traffic flow ends naturally, for example, stopped from the source. If the flow is re-initiated from a host, it will not be translated by the firewall, as the rule is deleted after the first flow stopped.

**Examples** To perform network address translation and port forward application 'http' from entity 'public' to any with target destination dmz.servers.web\_server, use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# rule 10 portfw
http from public with dst dmz.servers.web_server
```

To perform network address translation and masquerade application 'http' from entity 'private' to 'public', use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# rule 20 masq
http from private to public
```

To use subnet-based NAT to translate the source address of all traffic from 'private.lan' going to 'remote.lan' with the new subnet specified in 'private.global', use the commands:

```
awplus# configure terminal
awplus(config)# nat
awplus(config-nat)# rule 30 netmap all from private.lan to
remote.lan with src private.global
```

To remove NAT rule 10, use the command:

```
awplus(config-nat)# no rule 10
```

**Related  
commands**

[application](#)  
[clear firewall connections](#)  
[host \(network\)](#)  
[move rule \(nat\)](#)  
[nat](#)  
[network \(zone\)](#)  
[show nat rule](#)  
[show nat rule config-check](#)  
[show running-config nat](#)  
[zone](#)

**Command  
changes**

Version 5.4.7-0.1: **netmap** option added.

# show nat

**Overview** Use this command to show the configuration state of NAT.

**Syntax** `show nat`

**Mode** Privileged Exec

**Examples** To show the configuration state of NAT, use the commands:

```
awplus# show nat
```

**Output** Figure 57-2: Example output from the **show nat** command

```
awplus#show nat
NAT is enabled
```

**Related commands** [enable \(nat\)](#)

# show nat rule

**Overview** Use this command to show information about NAT rules.

**Syntax** show nat rule [<1-65535>]

| Parameter | Description |
|-----------|-------------|
| <1-65535> | Rule ID     |

**Mode** Privileged Exec

**Examples** To show information about all NAT rules, use the command:

```
awplus# show nat rule
```

**Output** Figure 57-3: Example output from the **show nat rule** command

```
awplus#show nat rule
```

| [* = Rule is not valid - see "show nat rule config-check"] |        |      |         |        |         |      |
|------------------------------------------------------------|--------|------|---------|--------|---------|------|
| ID                                                         | Action | App  | From    | To     | With    | Hits |
| -----                                                      |        |      |         |        |         |      |
| * 30                                                       | masq   | any  | private | public | -       | 0    |
| 10                                                         | portfw | http | public  | -      | dmz.a.b | 0    |

To show information about a specific NAT rule, use the command:

```
awplus# show nat rule 10
```

**Output** Figure 57-4: Example output from the **show nat rule** command

```
awplus#show nat rule 10
```

| [* = Rule is not valid - see "show nat rule config-check"] |        |      |        |    |         |      |
|------------------------------------------------------------|--------|------|--------|----|---------|------|
| ID                                                         | Action | App  | From   | To | With    | Hits |
| -----                                                      |        |      |        |    |         |      |
| 10                                                         | portfw | http | public | -  | dmz.a.b | 0    |

| Output Parameter | Description                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------------------|
| *                | Indicates the rule is not valid and cannot be hit, see the <a href="#">show nat rule config-check</a> command. |
| App              | Application name.                                                                                              |
| From             | Source entity.                                                                                                 |

| Output Parameter | Description                                    |
|------------------|------------------------------------------------|
| with             | Target entity name.                            |
| To               | Destination entity.                            |
| Hits             | The number of times the NAT rule has been hit. |

**Related commands**   [rule \(nat\)](#)  
[show nat rule config-check](#)



# show nat rule config-check

**Overview** Use this command to check configuration validity of NAT rules.

An invalid rule will not be active and cannot be hit.

This command also shows the reasons why a rule is not valid.

**Syntax** `show nat rule config-check`

**Mode** Privileged Exec

**Usage notes** NAT rules are applied to applications and entities. A rule is not valid if either the application, source entity or destination entity the rule applies to is not configured properly.

To configure applications and entities, see Application and Entity Commands.

**Examples** To check configuration validity of NAT rules, use the command:

```
awplus# show nat rule config-check
```

**Output** Figure 57-5: Example output from the **show nat rule config-check** command if rule configuration errors are detected

```
awplus#show nat rule config-check
Rule 10:
 Application does not have a protocol configured
 "From" entity does not exist
 "To" entity has no subnet or host addresses
```

**Output** Figure 57-6: Example output from the **show nat rule config-check** command if all rules are valid

```
awplus#show nat rule config-check
All rules are valid
```

# show running-config nat

**Overview** Use this command to show the configuration commands that have been used to configure NAT.

**Syntax** `show running-config nat`

**Mode** Privileged Exec

**Examples** To show the configuration commands that have been used to configure NAT, use the commands:

```
awplus# show running-config nat
```

**Output** Figure 57-7: Example output from the **show running-config nat** command

```
awplus#show running-config nat
nat
 rule 10 masq http from private to public
 rule 20 portfw http from public with dst dmz.servers.wb
 enable
!
```

# Part 9: Advanced Network Protection

# 58

# IPS Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure Intrusion Prevention System (IPS). For more information, see the [IPS Feature Overview and Configuration\\_Guide](#).

The table below lists the IPS commands and their applicable modes.

Figure 58-1: IPS Commands and Applicable Modes

| Mode                 | Command                              |
|----------------------|--------------------------------------|
| Privileged Exec      | <code>show ips</code>                |
|                      | <code>show ips categories</code>     |
|                      | <code>show running-config ips</code> |
| Global Configuration | <code>ips</code>                     |
| IPS Mode             | <code>alert-thresholding</code>      |
|                      | <code>category action (IPS)</code>   |
|                      | <code>protect (IPS)</code>           |

- Command List**
- [“alert-thresholding”](#) on page 2610
  - [“category action \(IPS\)”](#) on page 2611
  - [“ips”](#) on page 2612
  - [“protect \(IPS\)”](#) on page 2613
  - [“provider \(IPS\)”](#) on page 2614
  - [“show ips”](#) on page 2615
  - [“show ips categories”](#) on page 2616
  - [“show ips categories detail”](#) on page 2618

- [“show running-config ips”](#) on page 2620
- [“sid”](#) on page 2621
- [“update-interval \(IPS\)”](#) on page 2622

# alert-thresholding

**Overview** Use this command to limit IPS to a maximum of 6 alerts per minute per destination IP address. This prevents IPS alerts from overwhelming the log files.

Use the **no** variant of this command to turn off the limit if you need to log every packet that matches an IPS rule (for example, for debugging purposes).

**Syntax** alert-thresholding  
no alert-thresholding

**Default** Enabled

**Mode** IPS Configuration

**Example** To stop limiting the number of IPS alerts, so that the device logs every packet that matches an IPS rule, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no alert-thresholding
```

To limit the number of IPS alerts again, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# alert-thresholding
```

**Related commands** show log  
show ips

**Command changes** Version 5.5.0-2.1: command added

# category action (IPS)

**Overview** Use this command to configure an action for a specified category.

Use the **no** variant of this command to set the default action of alert for a specified category.

**Syntax** `category <category-name> action {alert|deny|disable}`  
`no category <category-name> action`

| Parameter                          | Description                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;category-name&gt;</code> | Category name. A category is a label that helps to classify the nature of traffic, for example, whether it is spammer, spot or spyware and so on. Once IPS protection is enabled, traffic will be categorized according to the available IPS categories. You can use the <a href="#">show ips categories</a> command to view the categories and their actions. |
| <code>alert</code>                 | Generate a log message. This is the default action.                                                                                                                                                                                                                                                                                                            |
| <code>deny</code>                  | Drop the matching packets. No error message is sent back to the source host.                                                                                                                                                                                                                                                                                   |
| <code>disable</code>               | Ignore a specified category. Ignored categories will not be used to categorize traffic.                                                                                                                                                                                                                                                                        |

**Default** The default action is alert.

**Mode** IPS Configuration

**Examples** To drop packets categorized as checksum, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# category checksum action deny
```

To set the default action for the category checksum, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no category checksum action
```

**Validation Commands** [show ips categories](#)  
[show running-config ips](#)

# ips

**Overview** Use this command to configure IPS.

Use the **no** variant of this command to remove all IPS configuration.

**Syntax** `ips`  
`no ips`

**Mode** Global Configuration

**Usage notes** This command allows you to enter the IPS mode. The command prompt for this mode is **awplus(config-ips)#**.

In the IPS mode, you can:

- Enable or disable IPS protection, see the [protect \(IPS\)](#) command.
- Configure an action for specified categories, see the [category action \(IPS\)](#) command.

**Examples** To configure IPS, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)#
```

To remove all IPS configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no ips
```



# protect (IPS)

**Overview** Use this command to enable IPS protection .  
Use the **no** variant of this command to disable IPS protection.

**Syntax** protect  
no protect

**Usage notes** Once IPS protection is enabled, traffic will be categorized according to the available IPS categories. See the [show ips categories](#) command for the list of available IPS categories.

**Default** IPS is disabled by default.

**Mode** IPS Mode

**Examples** To enable IPS protection, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# protect
```

To disable IPS protection, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no protect
```

**Validation  
Commands** [show ips](#)  
[show running-config ips](#)

# provider (IPS)

**Overview** Use this command to configure an IPS (Intrusion Prevention System) provider.

A provider is a third-party vendor that supplies a comprehensive rule set for detecting and blocking advanced threats.

Rule sets include extensive signatures. This is where a previously known event can be characterised in some way that can be used to detect if the event happens again. The signature database is kept up-to-date to ensure the effectiveness of the detection.

Use the **no** variant of this command to disable a provider.

**Syntax** `provider proofpoint`  
`no provider`

| Parameter  | Description                       |
|------------|-----------------------------------|
| proofpoint | Use Proofpoint signatures in IPS. |

**Mode** IPS Configuration

**Example** To configure Proofpoint as the provider, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# provider proofpoint
```

To unset a provider, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no provider
```

**Related commands** [show ips](#)  
[show running-config ips](#)

**Command changes** Version 5.5.2-2.1: command added

# show ips

**Overview** Use this command to show the IPS configuration state and event count for the Intrusion Prevention System (IPS).

**Syntax** `show ips`

**Mode** Privileged Exec

**Examples** To display information about IPS, use the command:

```
awplus# show ips
```

**Output** Figure 58-2: Example output from **show ips**

```
awplus#show ips
Status: Enabled (Active)
Events: 4
Alert Thresholding: Enabled
```

Table 58-1: Parameters in the output from **show ips**

| Parameter          | Description                                                                                                                                                                                                                                                  |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Alert Thresholding | Either Enabled or Disabled. When enabled, IPS produces a maximum of 6 alerts per minute per destination IP address. This prevents IPS alerts from overwhelming the log files. To enable or disable this, use the <a href="#">alert-thresholding</a> command. |

**Related commands** [show ips categories detail](#)

# show ips categories

**Overview** Use this command to show the IPS categories and their actions.

Note that if the IPS database provider is configured, this command shows only the provider's categories.

**Syntax** `show ips categories`

**Mode** Privileged Exec

**Examples** To show the IPS categories and their actions, use the command:

```
awplus# show ips categories
```

**Output** Figure 58-3: Example output of built-in categories from the **show ips categories** command

|                            |        |
|----------------------------|--------|
| awplus#show ips categories |        |
| Category (* = invalid)     | Action |
| -----                      |        |
| checksum                   | alert  |
| ftp-bounce                 | alert  |
| gre-decoder-events         | alert  |
| http-events                | alert  |
| icmp-decoder-events        | alert  |
| ip-decoder-events          | alert  |
| ppp-decoder-events         | alert  |
| smtp-events                | alert  |
| stream-events              | alert  |
| udp-decoder-events         | alert  |

| Parameter          | Description                                                                                                                                                                                                                                                                                                                                |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| checksum           | Invalid checksums, e.g. IPv4, TCPv4, UDPv4, ICMPv4, TCPv6, UDPv6, ICMPv6.                                                                                                                                                                                                                                                                  |
| ftp-bounce         | GPL FTP PORT bounce attempt.                                                                                                                                                                                                                                                                                                               |
| gre-decoder events | GRE anomalies, e.g. GRE packet too small, GRE wrong version, GRE v0 recursion control, GRE v0 flags, GRE v0 header too big, GRE v1 checksum present, GRE v1 routing present, GRE v1 strict source route, GRE v1 recursion control.                                                                                                         |
| http-events        | HTTP anomalies, e.g. HTTP unknown error, HTTP gzip decompression failed, HTTP request field missing colon, HTTP response field missing colon, HTTP invalid request chunk length, HTTP invalid response chunk length, HTTP status 100-Continue already seen, HTTP unable to match response to request, HTTP invalid server port in request. |

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| icmp-decoder- events | ICMP anomalies, e.g. IPv6 with ICMPv4 header, ICMPv4 packet too small, ICMPv4 unknown type, ICMPv6 truncated packet, ICMPv6 unknown version.                                                                                                                                                                                                                                                                                                                      |
| ip-decoder- events   | IPv4 and IPv6 anomalies, e.g. IPv4 packet too small, IPv4 header size too small, IPv4 wrong IP version, IPv6 packet too small, IPv6 duplicated Routing extension header, IPv6 duplicated Hop-By- Hop Options extension header, IPv6 DSTOPTS only padding, SLL packet too small, Ethernet packet too small, VLAN header too small, FRAG IPv4 Fragmentation overlap, FRAG IPv6 Packet size too large, IPv4-in-IPv6 invalid protocol, IPv6-in-IPv6 packet too short. |
| ppp-decoder-events   | PPP anomalies, e.g. PPP packet too small, PPP IPv6 too small, PPP wrong type, PPPoE wrong code, PPPoE malformed tags.                                                                                                                                                                                                                                                                                                                                             |
| smtp-events          | SMTP anomalies, e.g. SMTP invalid reply, SMTP max reply line length exceeded, SMTP TLS rejected, SMTP data command rejected.                                                                                                                                                                                                                                                                                                                                      |
| stream-events        | TCP anomalies, e.g. 3way handshake with ack in wrong dir, 3way handshake async wrong sequence, 3way handshake right seq wrong ack evasion, 4way handshake SYNACK with wrong ACK, STREAM CLOSEWAIT FIN out of window, STREAM ESTABLISHED SYNACK resend, STREAM FIN invalid ack, STREAM FIN1 ack with wrong seq, STREAM TIMEWAIT ACK with wrong seq, stream-events TCP packet too small, stream-events TCP duplicated option)                                       |
| udp-decoder- events  | UDP anomalies, e.g. UDP packet too small, UDP header length too small, UDP invalid header length.                                                                                                                                                                                                                                                                                                                                                                 |

# show ips categories detail

**Overview** Use this command to show the detailed information about IPS (Intrusion Prevention System) categories.

**Syntax** `show ips categories detail [<category-name>]`

| Parameter                          | Description                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;category-name&gt;</code> | Optional - enter a category name to only show information about a specific category. <ul style="list-style-type: none"><li>Category names are case sensitive and can be up to 64 characters long composed of printable ASCII characters.</li><li>A category is a label that helps to classify the nature of traffic, for example, whether it is spammer, bot, or spyware and so on.</li></ul> |

**Mode** Privileged Exec

**Example** To show detailed information about all the IPS categories, use the command:

```
awplus# show ips categories detail
```

**Output** Figure 58-4: Example output from **show ips categories detail**

| awplus#show ips categories detail |        |       |                                                                                                                                                                                                                                                                      |
|-----------------------------------|--------|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Category (* = invalid)            | Action | Rules | Description                                                                                                                                                                                                                                                          |
| 3coresec                          | alert  | 33    | IP block list signatures automatically generated from the 3CORESec team's Honeypots                                                                                                                                                                                  |
| activex                           | alert  | 242   | Signatures for protection against attacks on Microsoft ActiveX controls and exploits targeting vulnerabilities in ActiveX controls                                                                                                                                   |
| attack_response                   | alert  | 692   | Signatures to identify responses indicative of intrusion. Examples include but not limited to LMHost file download, presence of web banners and the detection of Metasploit Meterpreter kill command. These are designed to catch the results of a successful attack |
| botcc                             | alert  | 24    | (Bot Command and Control) Signatures that are autogenerated from several sources of known and confirmed active botnet and other Command and Control (C2) hosts. This category is updated daily. Primarily sourced from Shadowserver.org                              |
| ...                               |        |       |                                                                                                                                                                                                                                                                      |

**Example** To show detailed information about the IPS category 'activex', use the command:

```
awplus# show ips categories detail activex
```

**Output** Figure 58-5: Example output from **show ips categories detail activex**

```
awplus#show ips categories detail activex
Category (* = invalid) Action Rules Description

activex alert 242 Signatures for protection against
 attacks on Microsoft ActiveX controls
 and exploits targeting vulnerabilities
 in ActiveX controls
```

**Related commands** [category action \(IPS\)](#)  
[show ips categories](#)

**Command changes** Version 5.5.2-2.1: command added

# show running-config ips

**Overview** Use this command to show the configuration commands that have been used to configure IPS.

**Syntax** `show running-config ips`

**Mode** Privileged Exec

**Examples** To show the commands that have been used to configure IPS, use the command:

```
awplus# show running-config ips
```

**Output** Figure 58-6: Example output from the **show running-config ips** command

```
awplus#show running-config ips
ips
 protect
!
```



# sid

**Overview** Use this command to configure a rule's action via its Signature ID (SID). Rule actions default to their category action. For example, if the IPS category 'smtp-events' is set to 'deny', then you can configure the SID '2220006' to be disabled so that the signature is not blocked.

The IPS log contains the SID for each configured IPS category.

Use the **no** variant of this command to return a SID to using the category's configured action.

**Syntax** `sid <1-2147483647> action {alert|deny|disable}`  
`no sid <1-2147483647>`

| Parameter      | Description                                                                  |
|----------------|------------------------------------------------------------------------------|
| <1-2147483647> | The SID of the rule to override.                                             |
| alert          | Generate a log message, this is the default action.                          |
| deny           | Drop the matching packets. No error message is sent back to the source host. |
| disable        | No action will be taken for matching packets.                                |

**Default** Alert.

**Mode** IPS Configuration

**Example** To disable the IPS rule for SID 2220006, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# sid 2220006 action disable
```

To return the IPS rule for SID 2220006 back to the action of its category, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no sid 2220006 action
```

**Related commands** [show ips](#)  
[show running-config ips](#)

**Command changes** Version 5.5.2-2.1: command added

# update-interval (IPS)

**Overview** Use this command to configure an update check interval for the IPS provider resource files.

A provider is a third-party vendor that supplies a comprehensive rule set for detecting and blocking advanced threats.

Use the **no** variant of this command to use the default update interval of IPS provider resources.

**Syntax** `update-interval {minutes <10-525600>|hours <1-8760>|days <1-365>|weeks <1-52>|never}`  
`no update-interval`

| Parameter           | Description                                    |
|---------------------|------------------------------------------------|
| minutes <10-525600> | Update interval from 10 through 52600 minutes  |
| hours <1-8760>      | Update interval from 1 hour through 8760 hours |
| days <1-365>        | Update interval from 1 day through 365 days    |
| weeks <1-52>        | Update interval from 1 week through 52 weeks   |
| never               | Never update the resource.                     |

**Default** 1 hour.

**Mode** IPS Configuration

**Usage notes** The Update Manager will perform an update check for a resource when triggered by an update check interval. It will request the current version number of the resource from the Update Server, then compare it with the current local version. If they are different, the Update Manager will initiate an update of the local resource.

The Update Manager will revert to last known good resource file if installation of an updated resource fails.

Note that when a feature is disabled, regular and manual update checks for its resources are disabled.

Also note that an update check for a resource will not proceed if an update of that resource is already in progress.

**Example** To check and update the IPS provider resource files once a week, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# update-interval weeks 1
```

To disable updating the IPS provider resource files, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# update-interval never
```

To restore the default update interval for IPS provider resource files, use the commands:

```
awplus# configure terminal
awplus(config)# ips
awplus(config-ips)# no update-interval
```

**Related  
commands**

[show running-config ips](#)

**Command  
changes**

Version 5.5.2-2.1: command added

# 59

# Malware Protection Commands

## Introduction

This chapter provides an alphabetical reference of commands used to configure Malware Protection. For more information about Malware Protection and a configuration example, see the [Advanced Network Protection Feature Overview and Configuration Guide](#).

The table below lists the Malware Protection commands and their applicable modes.

Figure 59-1: Malware Protection commands and applicable modes

| Mode                    | Command                                             |
|-------------------------|-----------------------------------------------------|
| Privileged Exec         | <code>show malware-protection</code>                |
|                         | <code>show running-config malware-protection</code> |
| Global Configuration    | <code>malware-protection</code>                     |
| Malware Protection Mode | <code>protect (malware)</code>                      |
|                         | <code>provider kaspersky (malware)</code>           |
|                         | <code>update-interval (malware)</code>              |

- Command List**
- “[malware-protection](#)” on page 2625
  - “[protect \(malware\)](#)” on page 2626
  - “[provider kaspersky \(malware\)](#)” on page 2627
  - “[show malware-protection](#)” on page 2628
  - “[show running-config malware-protection](#)” on page 2629
  - “[update-interval \(malware\)](#)” on page 2630

# malware-protection

**Overview** Use this command to configure Malware Protection.

Use the **no** variant of this command to remove all Malware Protection configuration.

**Syntax** `malware-protection`  
`no malware-protection`

**Mode** Global Configuration

**Usage notes** This command allows you to enter the Malware Protection Mode. The command prompt for this mode is **awplus(config-malware)#**.

In the Malware Protection Mode, you can:

- Set the Malware Protection provider, see the [provider kaspersky \(malware\)](#) command.
- Enable or disable Malware Protection, see the [protect \(malware\)](#) command.

**Examples** To configure Malware Protection settings, use the commands:

```
awplus# configure terminal
awplus(config)# malware-protection
awplus(config-malware)#
```

To remove all Malware Protection configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no malware-protection
```

**Validation Commands** [show malware-protection](#)

# protect (malware)

**Overview** Use this command to enable Malware Protection.

Use the **no** variant of this command to disable Malware Protection without losing existing Malware Protection configuration.

Note that you need to use the [provider kaspersky \(malware\)](#) command to set Malware Protection provider before issuing this command to enable Malware Protection.

**Syntax** protect  
no protect

**Default** Malware Protection is disabled by default.

**Mode** Malware Protection Mode

**Examples** To enable Malware Protection, use the commands:

```
awplus# configure terminal
awplus(config)# malware-protection
awplus(config-malware)# provider kaspersky
awplus(config-malware)# protect
```

To disable Malware Protection, use the commands:

```
awplus# configure terminal
awplus(config)# malware-protection
awplus(config-malware)# no protect
```

**Validation Commands** [show malware-protection](#)  
[show running-config malware-protection](#)

**Related commands** [provider kaspersky \(malware\)](#)

# provider kaspersky (malware)

- Overview** Use this command to set Malware Protection provider.
- Malware Protection provider provides a signature database containing a list of known threat patterns. The database is kept up-to-date to ensure the effectiveness of the detection. You can use the [update-interval \(malware\)](#) command to configure the update check interval and update local database if needed.
- Note that you need to set Malware Protection provider before issuing [protect \(malware\)](#) command to enable Malware Protection.
- Syntax** `provider kaspersky`
- Default** No Malware Protection provider is set.
- Mode** Malware Protection Mode
- Examples** To set Malware Protection provider, use the commands:
- ```
awplus# configure terminal
awplus(config)# malware-protection
awplus(config-malware)# provider kaspersky
```
- Validation Commands** [show malware-protection](#)
[show running-config malware-protection](#)
- Related commands** [protect \(malware\)](#)

show malware-protection

Overview Use this command to show the information about the operation of Malware Protection.

Syntax `show malware-protection`

Mode Privileged Exec

Examples To show the operation of Malware Protection, use the command:

```
awplus# show malware-protection
```

Output Figure 59-2: Example output from **show malware-protection** if the subscription license for Malware Protection is active.

```
awplus#show malware-protection
Status:      Enabled (Active)
Events:      0
Provider:    Kaspersky
Resource version:      1.0
Resource update interval: 1 hour
```

Command changes Version 5.4.7-0.1: Event count added to the command output.

show running-config malware-protection

Overview Use this command to show the configuration information about Malware Protection.

Syntax `show running-config malware-protection`

Mode Privileged Exec

Examples To show the running configuration of Malware Protection, use the command:

```
awplus# show running-config malware-protection
```

Output Figure 59-3: Example output from the **show running-config malware-protection** command on the console

```
awplus#show running-config malware-protection
malware-protection
  provider kaspersky
  protect
!
```

update-interval (malware)

Overview Use this command to configure an update check interval for the Malware Protection resource files.

Use the **no** variant of this command to restore the default update check interval to 1 hour.

Syntax `update-interval {minutes <10-525600>|hours <1-8760>|days <1-365>|weeks <1-52>|never}`
`no update-interval`

Parameter	Description
minutes <10-525600>	Update interval from 10 through 525600 minutes
hours <1-8760>	Update interval from 1 hour through 8760 hours
days <1-365>	Update interval from 1 day through 365 days
weeks <1-52>	Update interval from 1 week through 52 weeks
never	Never update the resource. If Malware Protection becomes enabled, the Update Manager will do update check and update the resource files if needed. Use the protect (malware) command to enable Malware Protection.

Default The default update interval is 1 hour.

Mode Malware Protection Mode

Usage notes The Update Manager will perform an update check for a resource when triggered by an update check interval. It will request the current version number of the resource from the Update Server, then compare it with the current local version. If they are different, the Update Manager will initiate an update of the local resource.

The Update Manager will revert to last known good resource file if installation of an updated resource fails.

Note that when a feature is disabled, regular and manual update checks for its resources are disabled.

Also note that an update check for a resource will not proceed if an update of that resource is already in progress.

Examples To check and update the Malware Protection resource files once a week, use the command:

```
awplus(config-malware)# update-interval weeks 1
```

To disable updating of the resource, use the command:

```
awplus(config-malware)# update-interval never
```

To restore the default update interval, which is 1 hour, use the command:

```
awplus(config-malware)# no update-interval
```

Validation [show resource](#)
Commands

60

Antivirus Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Antivirus. For more information about Antivirus and its configuration, see the Antivirus sections contained within the [Advanced Network Protection Feature Overview and Configuration Guide](#).

The following table lists the Antivirus commands and their applicable modes.

Figure 60-1: Antivirus commands and applicable modes

Mode	Command
Privileged Exec	<code>show antivirus</code>
	<code>show antivirus statistics</code>
	<code>show running-config antivirus</code>
	<code>debug antivirus</code>
	<code>show debugging antivirus</code>
Global Configuration	<code>antivirus</code>
Antivirus Mode	<code>action (antivirus)</code>
	<code>protect (antivirus)</code>
	<code>provider kaspersky (antivirus)</code>
	<code>update-interval (antivirus)</code>

- Command List**
- “[action \(antivirus\)](#)” on page 2634
 - “[antivirus](#)” on page 2636
 - “[dpi categorize](#)” on page 2637
 - “[debug antivirus](#)” on page 2638

- [“protect \(antivirus\)”](#) on page 2639
- [“provider kaspersky \(antivirus\)”](#) on page 2640
- [“show antivirus”](#) on page 2641
- [“show antivirus statistics”](#) on page 2642
- [“show debugging antivirus”](#) on page 2643
- [“show running-config antivirus”](#) on page 2644
- [“update-interval \(antivirus\)”](#) on page 2645

action (antivirus)

Overview Use this command to set the action to take when a scan fails or when a scan limit is exceeded.

Use the **no** variant of this command to restore the default action, which is deny.

Syntax `action {scan-failed|limit-exceeded} {deny|permit}`
`no action {scan-failed|limit-exceeded}`

Parameter	Description
scan-failed	Scan failed for a wide variety of possible reasons, for example, encrypted or corrupt file type, out of temporary memory, license expired.
limit-exceeded	Scan failed due to a nesting limit or memory limit being exceeded. Antivirus can extract and scan nested files up to 3 levels deep. The maximum size of a file object that can be sent for scanning is 10MB. The maximum total size of all objects that can be concurrently scanned is 100MB.
deny	Block HTTP request.
permit	Allow HTTP request.

Default The default action is deny when a scan failed or a scan limit is exceeded.

Mode Antivirus Mode

Examples To allow HTTP traffic when a scan fails, use the commands:

```
awplus# configure terminal
awplus(config)# antivirus
awplus(config-antivirus)# action scan-failed permit
```

To block HTTP request when a scan fails, use the commands:

```
awplus# configure terminal
awplus(config)# antivirus
awplus(config-antivirus)# action scan-failed deny
```

To allow HTTP request when a scan limit is exceeded, use the commands:

```
awplus# configure terminal
awplus(config)# antivirus
awplus(config-antivirus)# action limit-exceeded permit
```

To block HTTP traffic when a scan limit is exceeded, use the commands:

```
awplus# configure terminal
awplus(config)# antivirus
awplus(config-antivirus)# action limit-exceeded deny
```

To restore the default action when a scan fails, use the commands:

```
awplus# configure terminal
awplus(config)# antivirus
awplus(config-antivirus)# no action scan-failed
```

To restore the default action when a scan limit is exceeded, use the commands:

```
awplus# configure terminal
awplus(config)# antivirus
awplus(config-antivirus)# no action limit-exceeded
```

Validation [show antivirus](#)
Commands

antivirus

Overview Use this command to configure Antivirus.

Use the **no** variant of this command to remove all Antivirus configuration.

Syntax `antivirus`
`no antivirus`

Mode Global Configuration

Usage notes This command allows you to enter the Antivirus Mode. The command prompt for this mode is **awplus(config-antivirus)#**.

In the Antivirus Mode, you can:

- Set the action to take if a scan failed or a scan limit is exceeded, see the [action \(antivirus\)](#) command.
- Enable or disable Antivirus protection, see the [protect \(antivirus\)](#) command.

Examples To configure Antivirus settings, use the commands:

```
awplus# configure terminal
awplus(config)# antivirus
awplus(config-antivirus)#
```

To remove all Antivirus configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no antivirus
```

**Validation
Commands** [show antivirus](#)

dpi categorize

Overview Use this command to determine the category that DPI will assign to a URL, when using DPI Web Categorization.

Syntax `dpi categorize <url-list>`

Parameter	Description
<code><url-list></code>	One or more website HTTP or HTTPS URLs, separated by a space. If neither 'http://' nor 'https://' is specified in the URL, the default 'http://' is automatically added.

Mode Privileged Exec

Usage notes When you use this command, you can see the category that the DPI Web Categorization provider has allocated for each URL.

This category can then be used when configuring features that use application matching.

Example To display the categorization for `www.google.com` and `www.bbc.co.uk`, use the commands:

```
awplus# configure terminal
awplus(config)# dpi categorize www.google.com www.bbc.co.uk
```

Output Figure 60-2: Example output from **dpi categorize**

```
awplus#dpi categorize www.google.com www.bbc.co.uk
http://www.google.com: search-engines
http://www.bbc.co.uk: news-media
```

Related commands [web-control categorize](#)
[web-categorization](#)

Command changes Version 5.5.2-2.1: command added

debug antivirus

Overview Use this command to enable Antivirus debugging. This will cause additional detailed debugging information to be logged at the “informational” and “debugging” levels.

Use the **no** variant of this command to disable Antivirus debugging.

Syntax debug antivirus
no debug antivirus

Default Antivirus debugging is disabled by default.

Mode Privileged Exec

Examples To enable Antivirus debugging, use the command:

```
awplus# debug antivirus
```

To disable Antivirus debugging, use the command:

```
awplus# no debug antivirus
```

**Validation
Commands** show debugging antivirus
show antivirus

protect (antivirus)

Overview Use this command to enable Antivirus protection.

Use the **no** variant of this command to disable Antivirus protection without losing existing Antivirus configuration.

Note that you need to use the [provider kaspersky \(antivirus\)](#) command to set Antivirus provider before issuing this command to enable Antivirus protection.

Syntax protect
no protect

Default Antivirus is disabled by default.

Mode Antivirus Mode

Examples To enable Antivirus protection, use the commands:

```
awplus# configure terminal
awplus(config)# antivirus
awplus(config-antivirus)# provider kaspersky
awplus(config-antivirus)# protect
```

To disable Antivirus protection, use the commands:

```
awplus# configure terminal
awplus(config)# antivirus
awplus(config-antivirus)# no protect
```

**Validation
Commands** [show antivirus](#)
[show running-config antivirus](#)

**Related
commands** [provider kaspersky \(antivirus\)](#)

provider kaspersky (antivirus)

Overview Use this command to set Antivirus provider.

Antivirus provider provides a signature database containing a list of known threat patterns. The database is kept up-to-date to ensure the effectiveness of the detection. You can use the [update-interval \(antivirus\)](#) command to configure the update check interval and update local database if needed.

Note that you need to set Antivirus provider before issuing [protect \(antivirus\)](#) command to enable Antivirus protection.

Syntax `provider kaspersky`

Default No Antivirus provider is set.

Mode Antivirus Mode

Examples To set Antivirus provider, use the commands:

```
awplus# configure terminal
awplus(config)# antivirus
awplus(config-antivirus)# provider kaspersky
```

**Validation
Commands** [show antivirus](#)
[show running-config antivirus](#)

**Related
commands** [protect \(antivirus\)](#)

show antivirus

Overview Use this command to show the information about the operation of Antivirus.

Syntax show antivirus

Mode Privileged Exec

Examples To show the operation of Antivirus, use the command:

```
awplus# show antivirus
```

Output Figure 60-3: Example output from the **show antivirus** command on the console if the subscription license of Antivirus is active.

```
Status:      Enabled (Active)
Provider:    Kaspersky
Scan failed action:  block
Limit exceeded action: block
Resource version:    1.0
Resource update interval: 1 hour
```

Figure 60-4: Example output from the **show antivirus** command on the console if the subscription license of Antivirus is inactive.

```
awplus#show antivirus
Status:      Enabled (Inactive Unlicensed)
Provider:    Kaspersky
Scan failed action:  block
Limit exceeded action: block
Resource version:    not set
Resource update interval: 1 hour
```

show antivirus statistics

Overview Use this command to show Antivirus statistics.

Syntax show antivirus statistics

Mode Privileged Exec

Examples To show Antivirus statistics, use the command:

```
awplus# show antivirus statistics
```

Output Figure 60-5: Example output from the **show antivirus statistics** command

```
awplus#show antivirus statistics
Proxy Antivirus Statistics:
Files scanned:      1572
Files skipped:      0
Viruses found:      3 (0.2%)
Scan failures:      0 (0.0%)
Limit exceeded:     0 (0.0%)
```

Output Parameter	Description
Files scanned	The number of files that have been scanned.
Files skipped	The number of files that could not be scanned.
Viruses found	The number of files that contain a virus. Also shown as a percentage of total number of scanned files.
Scan failures	The number of times a scan failed. Also shown as a total number of scans.
Limit exceeded	The number of times a scan limit is exceeded. Also shown as a total number of scans.

show debugging antivirus

Overview Use this command to see what debugging is turned on for Antivirus.

Syntax show debugging antivirus

Mode Privileged Exec

Examples To show the Antivirus debugging setting, use the command:

```
awplus# show debugging antivirus
```

Output Figure 60-6: Example output from the **show debugging antivirus** command

```
awplus#show debugging antivirus
Antivirus Debugging Status: on
```

Related commands [debug antivirus](#)

show running-config antivirus

Overview Use this command to show the configuration information about Antivirus.

Syntax `show running-config antivirus`

Mode Privileged Exec

Examples To show the running configuration of Antivirus, use the command:

```
awplus# show running-config antivirus
```

Output Figure 60-7: Example output from the **show running-config antivirus** command

```
awplus#show running-config antivirus
antivirus
  provider kaspersky
  action scan-failed permit
  update-interval weeks 1
  protect
!
```


update-interval (antivirus)

Overview Use this command to configure an update check interval for the Antivirus resource files.

Use the **no** variant of this command to restore the default update check interval to 1 hour.

Syntax `update-interval {minutes <10-525600>|hours <1-8760>|days <1-365>|weeks <1-52>|never}`
`no update-interval`

Parameter	Description
minutes <10-525600>	Update interval from 10 through 52600 minutes
hours <1-8760>	Update interval from 1 hour through 8760 hours
days <1-365>	Update interval from 1 day through 365 days
weeks <1-52>	Update interval from 1 week through 52 weeks
never	Never update the resource. If Antivirus becomes enabled, the Update Manager will do update check and update the resource files if needed. Use the protect (antivirus) command to enable Antivirus.

Default The default update interval is 1 hour.

Mode Antivirus Mode

Usage notes The Update Manager will perform an update check for a resource when triggered by an update check interval. It will request the current version number of the resource from the Update Server, then compare it with the current local version. If they are different, the Update Manager will initiate an update of the local resource.

The Update Manager will revert to last known good resource file if installation of an updated resource fails.

Note that when a feature is disabled, regular and manual update checks for its resources are disabled.

Also note that an update check for a resource will not proceed if an update of that resource is already in progress.

Examples To check and update the Antivirus resource files once a week, use the command:

```
awplus(config-antivirus)# update-interval weeks 1
```

To disable updating of the resource, use the command:

```
awplus(config-antivirus)# update-interval never
```

To restore the default update interval, which is 1 hour, use the command:

```
awplus(config-antivirus)# no update-interval
```

Validation [show resource](#)
Commands

61

URL Filtering Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure URL filtering.

URL filtering blocks all HTTP and HTTPS access to a list of websites. You can either specify a short list of websites to block (up to 1000 blacklist and 1000 whitelist rules), or subscribe to a blacklist service offered by a third-party provider.

If you subscribe to a blacklist service, you can create custom blacklists to block additional URLs not in the third-party provider's blacklist or custom whitelists to allow URLs that the service blocks.

URL filtering blocks all HTTP and HTTPS access to a list of websites. You can specify a short list of websites (up to 1000 blacklist and 1000 whitelist rules) using custom blacklists to block URLs and custom whitelists to allow access to URLs.

For more information, see the [URL Filtering Feature Overview_and Configuration Guide](#).

The following table lists the URL filtering commands and their applicable modes.

Figure 61-1: URL filtering commands and applicable modes

Mode	Command
Privileged Exec	show running-config url-filter
	show url-filter
	url-filter reload custom-lists
Global Configuration	url-filter

Mode	Command
URL Filter Configuration	blacklist
	protect (url-filter)
	provider kaspersky (url-filter)
	update-interval (url-filter)
	whitelist (url-filter)

- Command List**
- [“blacklist”](#) on page 2649
 - [“log url-requests”](#) on page 2650
 - [“protect \(url-filter\)”](#) on page 2651
 - [“provider kaspersky \(url-filter\)”](#) on page 2652
 - [“show running-config url-filter”](#) on page 2653
 - [“show url-filter”](#) on page 2654
 - [“update-interval \(url-filter\)”](#) on page 2655
 - [“url-filter reload custom-lists”](#) on page 2657
 - [“url-filter”](#) on page 2658
 - [“whitelist \(url-filter\)”](#) on page 2659

blacklist

Overview Use this command to add a custom blacklist file to the URL filtering configuration. Use the **no** variant of this command to remove a blacklist from the URL filtering configuration.

Syntax `blacklist <location_of_blacklist_file>`
`no blacklist <location_of_blacklist_file>`

Parameter	Description
<code><location_of_blacklist_file></code>	Location of the blacklist file.

Mode URL Filter Configuration

Usage notes You can use custom blacklists to specify URLs to be blocked. If you are using the Kaspersky service, custom blacklists are processed before the Kaspersky blacklist. For information about blacklist rule format, see the [URL Filtering Feature Overview and Configuration Guide](#). You can use the [whitelist \(url-filter\)](#) command to add a whitelist that will override any corresponding blacklist entries.

Examples

Related commands [protect \(url-filter\)](#)
[show url-filter](#)
[url-filter reload custom-lists](#)
[whitelist \(url-filter\)](#)

log url-requests

Overview If URL Filtering is enabled, then by default, black list hits and issues with match criteria and list files are logged.

Use this command to enable logging of all HTTP and HTTPS URL requests (both permitted and denied) passing through the firewall.

Use the **no** variant of this command to disable extra logging of HTTP and HTTPS URL requests passing through the firewall.

Syntax `log url-requests`
`no log url-requests`

Default Disabled by default.

Mode URL Filter Configuration

Usage notes When enabled, additional log messages for HTTP and HTTPS URL requests passing through the firewall contain the:

- URL being accessed
- IP address of the user that requested the URL

Example To configure logging of all HTTP and HTTPS URL requests passing through the firewall (permitted as well as denied), use the following commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# log url-requests
```

Related commands [url-filter](#)

Command changes Version 5.4.7-1.1: command added

protect (url-filter)

Overview Use this command to enable URL filter protection.

Use the **no** variant of this command to disable URL filter protection without losing the existing URL filter configuration.

Syntax protect
no protect

Default URL filter protection is disabled by default and all HTTP and HTTPS traffic is allowed.

Mode URL Filter Configuration

Usage notes If you are subscribed to the Kaspersky service, you must enter the [provider kaspersky \(url-filter\)](#) command before entering this command.

Examples To enable URL filter protection, use the commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# provider kaspersky
awplus(config-url-filter)# protect
```

To disable URL filter protection, use the commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# no protect
```

Related commands [provider kaspersky \(url-filter\)](#)
[show url-filter](#)

Command changes Version 5.4.7-1.1: HTTPS support added.

provider kaspersky (url-filter)

Overview Use this command to set Kaspersky as the URL filter blacklist provider, and register Kaspersky's blacklist file with the update manager. This feature requires a Kaspersky subscription. For more information on Kaspersky see their website <https://support.kaspersky.com>

Syntax `provider kaspersky`

Mode URL Filter Configuration

Usage notes Kaspersky provides constantly updated blacklists that can be used for URL filtering. An HTTP or HTTPS request that includes a URL that matches an entry in the blacklist will be dropped.

NOTE: *that if you are using the Kaspersky service, you must enter this command before enabling URL filtering with the **protect** command.*

Examples To configure Kaspersky as the URL filter blacklist provider and then enable URL filtering, use the commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)# provider kaspersky
awplus(config-url-filter)# protect
```

Related commands [protect \(url-filter\)](#)
[show url-filter](#)

Command changes Version 5.4.7-1.1: HTTPS support added.

show running-config url-filter

Overview Use this command to show the running configuration information for URL filtering

Syntax `show running-config url-filter`

Mode Privileged Exec

Examples To show the running configuration of URL filtering, use the command:

```
awplus# show running-config url-filter
```

Output Figure 61-2: Example output from the **show running-config url-filter** command

```
awplus#show running-config url-filter
url-filter
  provider kaspersky
  protect
!
```

show url-filter

Overview Use this command to show information about the configuration state of URL filtering.

Syntax `show url-filter`

Mode Privileged Exec

Examples To show information about the configuration state of URL filtering, use the command:

```
awplus# show url-filter
```

Output Figure 61-3: Example output from **show url-filter**

```
awplus#show url-filter

Status:      Enabled (Active)
Events:      104
Custom blacklists  Entries
blacklist-example.txt  365
Custom whitelists  Entries
whitelist-example.txt  4
```

Output Figure 61-4: Example output from **show url-filter** if the Kaspersky URL blacklist subscription license is active.

```
awplus#show url-filter

Status:      Enabled (Active)
Provider:    Kaspersky
Status:      Enabled (Active)
Events:      104
Resource version:  1.0
Update interval:   1 hour
Blacklist entries: 63457
Custom blacklists  Entries
blacklist-example.txt  3
Custom whitelists  Entries
whitelist-example.txt  1
```

Command changes Version 5.4.7-0.1: Event count added to the command output.

update-interval (url-filter)

Overview Use this command to configure the update-interval for the URL filter provider blacklist resource file.

Use the **no** variant of this command to restore the default update check interval of 1 hour.

Syntax `update-interval {minutes <10-525600>|hours <1-8760>|days <1-365>|weeks <1-52>|never}`

`no update-interval`

Parameter	Description
minutes <10-525600>	Update interval from 10 through 52600 minutes
hours <1-8760>	Update interval from 1 hour through 8760 hours
days <1-365>	Update interval from 1 day through 365 days
weeks <1-52>	Update interval from 1 week through 52 weeks
never	Never update the resource. When URL filtering protection is enabled, the update manager will do an update check and update the resource files if necessary. Use the protect (url-filter) command to enable URL filtering protection.

Default The default update interval is 1 hour.

Mode URL Filter Configuration

Usage notes The update manager will perform an update check for a resource when triggered by an update check interval. It will request the current version number of the resource from the update server, then compare it with the current local version. If they are different, the update manager will initiate an update of the local resource.

The update manager will revert to the last known good resource file if installation of an updated resource fails.

Note that when a feature is disabled, regular and manual update checks for its resources are also disabled.

Also note that an update check for a resource will not proceed if an update of that resource is already in progress.

Examples To check and update the URL filter provider blacklist every 3 hours, use the command:

```
awplus(config-url-filter)# update-interval hours 3
```

To disable updating of the provider blacklist, use the command:

```
awplus(config-url-filter)# update-interval never
```

To configure resource update checking for URL filter to the default interval, which is 1 hour, use the command:

```
awplus(config-url-filter)# no update-interval
```

**Related
commands**

- [protect \(url-filter\)](#)
- [show resource](#)

url-filter reload custom-lists

Overview Use this command to reload all custom blacklists and whitelists after editing one or more of them.

Syntax `url-filter reload custom-lists`

Mode Privileged Exec

Examples To reload all custom blacklists and whitelists, use the following command:

```
awplus# url-filter reload custom-lists
```

Related commands [blacklist](#)
[whitelist \(url-filter\)](#)

url-filter

Overview Use this command to enter URL Filter Configuration mode and configure URL filtering functionality.

Use the **no** variant of this command to remove all URL filtering configuration.

Syntax `url-filter`
`no url-filter`

Mode Global Configuration

Usage notes This command allows you to enter the URL Filter Configuration mode and changes the command prompt to **awplus(config-url-filter)#**.

The URL Filter Configuration mode enables you to:

- Enable URL filtering protection; see the [protect \(url-filter\)](#) command.
- Configure the provider blacklist; see the [provider kaspersky \(url-filter\)](#) command.
- Configure custom blacklists; see the [blacklist](#) command.
- Configure custom whitelists; see the [whitelist \(url-filter\)](#) command.

Examples To enter the URL Filter Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# url-filter
awplus(config-url-filter)#
```

To remove all URL filter configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no url-filter
```

Related commands [blacklist](#)
[protect \(url-filter\)](#)
[provider kaspersky \(url-filter\)](#)
[show running-config](#)
[show url-filter](#)
[whitelist \(url-filter\)](#)

whitelist (url-filter)

Overview Use this command to add a custom whitelist file to the URL filtering configuration. Use the **no** variant of this command to remove a whitelist from the URL filter configuration.

Syntax `whitelist <url_of_whitelist_file>`
`no whitelist <location_of_whitelist_file>`

Parameter	Description
<code><location_of_whitelist_file></code>	Location of the whitelist file.

Mode URL Filter Configuration

Usage notes Whitelist matching precedes blacklist matching. You can use custom whitelists to override any corresponding blacklist entries. An HTTP or HTTPS request that includes a URL that matches an entry in a whitelist will be permitted.

For information about whitelist rule format, see the [URL Filtering Feature Overview and Configuration Guide](#).

Examples

Related commands `blacklist`
`protect (url-filter)`
`show url-filter`
`url-filter reload custom-lists`

Command changes Version 5.4.7-1.1: HTTPS support added.

62

Web Control Commands

Introduction

This chapter provides an alphabetical reference of commands used to configure Web Control. For more information, see the Web Control sections contained within the [Advanced Network Protection Feature Overview and Configuration_Guide](#).

The table lists the Web Control commands and their applicable modes.

Figure 62-1: Web Control commands and applicable modes

Mode	Command
Privileged Exec	<code>debug web-control</code>
	<code>show web-control</code>
	<code>show web-control categories</code>
	<code>show debugging web-control</code>
	<code>show running-config web-control</code>
	<code>show web-control rules</code>
Global Configuration	<code>web-control</code>
Web Control Configuration	<code>action (web-control)</code>
	<code>category (web-control)</code>
	<code>provider (web-control)</code>
	<code>protect (web-control)</code>
	<code>rule (web-control)</code>
	<code>move rule (web-control)</code>
Web Control Category Configuration mode	<code>match (web-control)</code>

Command List • [“action \(web-control\)” on page 2662](#)

- ["bypass-web-control entity"](#) on page 2663
- ["category \(web-control\)"](#) on page 2665
- ["debug web-control"](#) on page 2667
- ["match \(web-control\)"](#) on page 2668
- ["move rule \(web-control\)"](#) on page 2670
- ["protect \(web-control\)"](#) on page 2671
- ["provider \(web-control\)"](#) on page 2672
- ["rule \(web-control\)"](#) on page 2673
- ["show debugging web-control"](#) on page 2675
- ["show running-config web-control"](#) on page 2676
- ["show web-control"](#) on page 2677
- ["show web-control bypass"](#) on page 2679
- ["show web-control categories"](#) on page 2680
- ["show web-control rules"](#) on page 2682
- ["web-control"](#) on page 2683
- ["web-control categorize"](#) on page 2685

action (web-control)

Overview Use this command to set the action to take on uncategorized websites and categorized websites that don't hit any rule.

Use the **no** variant of this command to restore the default action which is deny.

Syntax `action {permit|deny}`
`no action`

Parameter	Description
permit	Allow access
deny	Block access

Default The default action is deny.

Mode Web Control Configuration

Examples To allow HTTP and HTTPS requests when no rules are hit, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# action permit
```

To restore the default action and block all HTTP and HTTPS requests when no rules are hit, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# no action
```

Related commands [show web-control](#)

Command changes Version 5.4.7-1.1: HTTPS support added.

bypass-web-control entity

Overview Use this command to allow traffic from a specific entity to bypass all web-control processing.

Use the **no** variant of this command to remove the web-control bypass for a specific entity.

Syntax `bypass-web-control <entity>`
`no bypass-web-control <entity>`

Parameter	Description
<code><entity></code>	The entity (zone, network, or host) which will not be processed by web-control. You can use the tab key to auto-complete entity names.

Default All traffic is processed by web-control.

Mode Privileged Exec

Usage notes This command is useful, if you know that a specific server IP is safe for applications requiring this bypass feature to be configured.

For example, this command is useful to allow an application that connects using HTTPS port 443 but does not actually send HTTPS data over that port connection, leading to the connection being blocked, due to the suspect nature of the application data transported via that port. This command can therefore introduce security risk if used improperly, so should be used sparingly.

Example If the following **entity** has been configured:

```
!  
zone server  
  network my  
  host box  
    ip address 192.168.2.2  
!
```

Then, you can create a web-control bypass for the entity **server.my.box**, using the following commands:

```
awplus# configure terminal  
awplus(config)# web-control  
awplus(config-web-control)# bypass-web-control server.my.box
```

Related commands [show web-control bypass](#)

Command changes Version 5.4.7-1.1: command added.

category (web-control)

Overview Use this command to configure a category.

A category is a text string that represents a logical grouping of websites. For example "Blog" is the category given to URLs that link to websites that are classified as being associated with blogging. There are two types of category: provider categories and custom categories. Provider categories are pre-defined categories. Digital Arts provides and constantly updates about 100 provider categories. Custom categories are defined by the users.

Use the **no** variant of this command to delete a custom category and delete all its match criteria.

NOTE: You cannot delete a provider category, but you can use the **no** variant of this command to delete the custom match criteria from the provider category.

Syntax `category <category-name>`
`no category <category-name>`

Parameter	Description
<code><category-name></code>	Category name. Category names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Spaces are allowed in category names, but the category names must be enclosed in double quotes ("").

Mode Web Control Configuration

Usage notes You can use the to display both provider categories and custom categories.

You cannot delete the provider categories or modify their names, but you can configure custom match criteria for provider categories. Custom match criteria precede and override provider categorization. This means if a website matches the match criteria from custom categories, the website will not be further categorized by Digital Arts.

This command allows you to enter the Web Control Category Configuration mode with the prompt **awplus(config-category)#**. You can create a set of match criteria for a category in this sub-mode. The match criteria are applied to website URLs as a simple string comparison. For more information about match criteria, see the [match \(web-control\)](#) command.

You can also create a set of rules for a category. Rules set the action to take for an HTTP or HTTPS request from a specific entity. For more information about rules, see the [rule \(web-control\)](#) command. For more information about entities, see the [Application and Entity Commands](#) chapter.

Examples To create a custom category named `work` and create match criteria for this category, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# category work
awplus(config-category)# match alliedtelesis
awplus(config-category)# match example
awplus(config-category)# match www.ietf.org
```

To delete the custom category and its match criteria, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# no category work
```

Related commands

- `match (web-control)`
- `rule (web-control)`
- `show web-control categories`

Command changes Version 5.4.7-1.1: HTTPS support added.

debug web-control

Overview Use this command to enable Web Control debugging. This will cause additional detailed debugging information to be logged at the “informational” and “debugging” levels.

Use the **no** variant of this command to disable Web Control debugging.

Syntax `debug web-control`
`no debug web-control`

Default Web Control debugging is disabled by default.

Mode Privileged Exec

Examples To enable Web Control debugging, use the commands:

```
awplus# debug web-control
```

To disable Web Control debugging, use the commands:

```
awplus# no debug web-control
```

Related commands [show debugging web-control](#)

match (web-control)

Overview Use this command to add a match criterion for a category.

A match criterion is a static string that is compared to a website URL (domain name or IP address) for a partial or complete match. A URL will be searched to see if it contains the given match criterion string. If the URL contains the string, then the match criterion is matched.

Note that the match criterion is not applied to the web page content.

Use the **no** variant of this command to delete a match criterion.

NOTE: If a custom category's last match criterion is deleted, then the category is automatically deleted.

Syntax `match <word>`
`no match <word>`

Parameter	Description
<code><word></code>	A string that is used to compare with IP addresses or domain names.

Mode Web Control Category Configuration

Usage notes Match criteria are case-insensitive and matched up to the first appearance of '?' (query string marker) or '#' (fragment identifier) in a website URL. For example, URL www.alliedtelesis.com/search.aspx?keyword=routers does not match the match criterion `match router` but www.alliedtelesis.com/routers does match that criterion.

When a URL matches a match criterion, the URL is categorized to the match criterion's category. A URL can be matched to more than one category. Custom match criteria override and precede provider categorization. If a URL or website matches custom criteria, then the URL will not be further sent for categorization by the provider criteria.

You can create up to 50 match criteria in total, so a category can have a maximum of 50 match criteria, or 50 categories can each have one match criterion, as long as the total number of the match criteria does not exceed 50.

For more information about categories, see the [category \(web-control\)](#) command.

Examples To create a match criterion with a string `ietf` for category `work`, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# category work
awplus(config-category)# match ietf
```


To delete a match criterion, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# category work
awplus(config-category)# no match ietf
```

To create a set of match criteria for category `movie`, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# category movie
awplus(config-category)# match youtube
awplus(config-category)# match imdb
awplus(config-category)# match rottentomatoes
```

Related commands [category \(web-control\)](#)
[show web-control categories](#)

move rule (web-control)

Overview Use this command to change the order of the Web Control rules. Note that a change to the rule order may change the Web Control results.

Syntax `move rule <1-65535> to <1-65535>`

Parameter	Description
<code>move rule <1-65535></code>	Move the ID of a given rule. The rule ID of the given rule must exist. Each rule has an ID which is either designated by the user or automatically generated when the rule is created. The rule ID is an integer from 1 to 65535.
<code>to <1-65535></code>	New rule ID to assign. The new rule ID must not be used by any existing rule.

Mode Web Control Configuration

Usage notes If a website is categorized into multiple categories because they have overlapping match criteria that have associated rules, only the rule with the lowest ID is applied. For example, a website is categorized into both category A associated with rule ID 1 and category B associated with ID 2. In this case, only category A's rule with ID 1 is applied to the website. To see the rule IDs, use the [show web-control rules](#) command.

You can move an existing rule ID only to an ID that is not assigned to any rule, otherwise you will be given an error message.

Examples To change the ID of a rule from 20 to 10, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# move rule 20 to 10
```

Related commands [rule \(web-control\)](#)
[show web-control rules](#)

protect (web-control)

Overview Use this command to enable Web Control protection.

Use the **no** variant of this command to disable Web Control protection without losing existing Web Control configuration.

Syntax protect
no protect

Default Web Control protection is disabled by default.

Mode Web Control Configuration

Usage notes Web Control protection is disabled and all HTTP and HTTPS traffic is allowed by default. You must issue the [provider \(web-control\)](#) command to configure the categorization provider before using this command.

Examples To enable Web Protection protection, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# provider digitalarts
awplus(config-web-control)# protect
```

To disable Web Control protection, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# no protect
```

Related commands [provider \(web-control\)](#)
[show web-control](#)

Command changes Version 5.4.7-1.1: HTTPS support added.

provider (web-control)

Overview Use this command to set Digital Arts or OpenText as the website categorization provider.

Syntax `provider [digitalarts|opentext]`

Mode Web Control Configuration

Usage notes Digital Arts provides about 100 pre-defined categories, and OpenText about 80 pre-defined categories. You can use the [show web-control categories](#) command to display the list of categories. For more information about categories, see the [category \(web-control\)](#) command.

Note that Web Control protection cannot be enabled by using the [protect \(web-control\)](#) command until the provider is configured.

Example To configure Digital Arts as the website categorization provider, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)# provider digitalarts
awplus(config-web-control)# protect
```

Related commands [protect \(web-control\)](#)
[show web-control](#)

Command changes Version 5.5.3-0.1: **opentext** parameter added

rule (web-control)

Overview Use this command to create a Web Control rule for a category.

Use the **no** variant of this command to remove a rule.

Syntax `rule [<rule-ID>] {permit|deny} <category> from <entity>`
`no rule <1-65535>`

Parameter	Description
<rule-ID>	Rule ID in the range from 1 through 65535. If you don't designate a rule ID, a rule ID will be automatically generated and it will be greater than the current highest rule ID.
permit	Set the rule's action to permit the access.
deny	Set the rule's action to block the access.
<category>	Website category that the rule applies to. Use the keyword any to apply the rule to all categories. This allows you to apply Web Control on a per entity basis. See the Advanced Network Protection Feature Overview and Configuration Guide for configuration examples.
<entity>	Source entity the rule applies to. Entity is a high level abstraction of a network device, a group of networks or subnets. For more information about entities, see Application and Entity Commands . You can use the tab key to auto-complete entity names.

Mode Web Control Configuration

Usage notes A rule sets the action to take if a website matches one or more of the match criteria of the rule's category and the request's source matches the entity the rule applies to. You may create multiple rules for a category. If the request does not hit the first rule, then the request is assessed against the next. If the request does not hit any rule, then the action set by the [action \(web-control\)](#) command is taken. The default action Web Control performs for uncategorized websites and categorized websites that do not match a rule is to deny.

A rule's action can either deny or permit an HTTP or HTTPS request. If a request hits a rule with a permit action, then the HTTP or HTTPS traffic of that website is allowed to pass through the device. If a request hits a rule with a deny action, then the HTTP or HTTPS traffic of that website is blocked and the client gets a notification page.

Entities represent logical groupings of subnets, hosts or interfaces. For more information about entities, see [Application and Entity Commands](#).

Rules are applied in order. Each rule has an ID which is either designated by the user or automatically generated. If a website is categorized into multiple categories because they have overlapping match criteria that have associated rules, only the rule with the lowest ID is applied. For example, a website is categorized into two categories: category A and category B. The rules for category A is allow, and for B is deny. If the rule ID of category A is lower than category B's, then the action allow is applied. To see the rule IDs, use the [show web-control rules](#) command.

You can change the rule order by using the [move rule \(web-control\)](#) command. A change to the rule order may change the Web Control results.

Examples To create a rule that blocks the entity called 'engineer' from accessing websites categorized as 'movie', use the commands:

```
awplus(config-web-control)# category movie
awplus(config-category)# match youtube
awplus(config-category)# match imdb
awplus(config-category)# exit
awplus(config-web-control)# rule 10 deny movie from engineer
```

To create a rule that allows the entity called 'engineer' to access category 'work', use the commands:

```
awplus(config-web-control)# category work
awplus(config-category)# match alliedtelesis
awplus(config-category)# exit
awplus(config-web-control)# rule permit work from engineer
```

To delete a rule, use the commands:

```
awplus(config-web-control)# no rule 10
```

To create a rule using the reserved keyword **any**:

```
awplus(config-web-control)# rule deny badsites from private
awplus(config-web-control)# rule permit any from private
```

Rules are processed in order. In the example above, the deny rule will block access to URLs associated with the named category 'badsites' from the named firewall entity 'private'. The subsequent 'permit any' rule will allow access to all other URLs originating from that specific firewall entity.

Related commands

- [show running-config](#)
- [show running-config web-control](#)
- [show web-control categories](#)
- [show web-control rules](#)

Command changes

- Version 5.4.7-1.1: HTTPS support added.
- Version 5.4.6-2.1: New category keyword 'any' added.

show debugging web-control

Overview Use this command to show the Web Control debugging status.

Syntax `show debugging web-control`

Mode Privileged Exec

Examples To show the Web Control debugging status, use the command:

```
awplus# show debugging web-control
```

Output Figure 62-2: Example output from the **show debugging web-control** command

```
awplus#show debugging web-control
Web Control Debugging Status: on
```

Related commands [debug web-control](#)

show running-config web-control

Overview Use this command to show the configuration information about Web Control.

Syntax `show running-config web-control`

Mode Privileged Exec

Examples To show the running configuration of Web Control, use the command:

```
awplus# show running-config web-control
```

Output Figure 62-3: Example output from **show running-config web-control**

```
awplus#show running-config web-control
web-control
  provider digitalarts
  protect
!
```

Related commands

- [rule \(web-control\)](#)
- [show running-config](#)
- [show web-control](#)
- [web-control](#)

show web-control

Overview Use this command to display the information about the state of Web Control.

Syntax show web-control

Mode Privileged Exec

Examples To show the Web Control configuration, use the command:

```
awplus# show web-control
```

Output Figure 62-4: Example output from the **show web-control** command if the subscription license of Web Control is active.

```
awplus#show web-control
Web Control protection is enabled
Web Control default action is deny
Web Control is licensed
Categorization provider is Digital Arts
Statistics:
  Categorization hits: 40/40  (100.0%)
  Rule hits:         20/40  (50.0%)
  Cache hits:       30/40  (75.0%)
  Cache size:       40
```

Figure 62-5: Example output from the **show web-control** command if the subscription license of Web Control is inactive.

```
awplus#show web-control
Web Control protection is enabled
Web Control default action is deny
Web Control is unlicensed
Categorization provider is Digital Arts
Statistics:
  Categorization hits: 0/0  (0.0%)
  Rule hits:         0/0  (0.0%)
  Cache hits:       0/0  (0.0%)
  Cache size:       0
```

Output Parameter for Statistics	Description
Categorization hits	The number of times the categories have been hit divided by the total number of HTTP and HTTPS requests.
Rule hits	The number of times the rules have been hit divided by the total number of requests.

Output Parameter for Statistics	Description
Cache hits	The number of times the cached websites have been hit divided by the total number of request to the cache.
Cache size	The number of websites that are currently cached in the system.

Related commands

- [rule \(web-control\)](#)
- [show running-config](#)
- [show running-config web-control](#)
- [show web-control categories](#)
- [web-control](#)

show web-control bypass

Overview Use this command to display information about all web-control bypasses.

Syntax show web-control bypass

Mode Privileged Exec

Example To display web-control bypass information, use the following commands:

```
awplus# configure terminal
awplus(config)# show web-control bypass
```

Output Figure 62-6: Example bypass configuration and output from **show web-control bypass**

```
!
zone server
network my
host box
ip address 192.168.2.2
!
!
web-control
action permit
provider digitalarts
bypass-web-control server.my.box
protect
!
awplus#show web-control bypass
Entity Name                               Bypass Hits
-----
server.my.box                             20
```

Related commands [bypass-web-control entity](#)

Command changes Version 5.4.7-1.1: command added.

show web-control categories

Overview Use this command to display all Web Control categories, including custom and provider categories.

For more information about categories, see the [category \(web-control\)](#) command.

Syntax `show web-control categories`

Mode Privileged Exec

Examples To show all Web Control categories, use the command:

```
awplus# show web-control categories
```

Output Figure 62-7: Example output from the **show web-control categories** command

Category	Category Hits	Custom
Custom Matches		

Advertisement	0	yes
AdWords		
YellowPages		
Advocacy	0	
"Alcohol, Tobacco"	0	
"Amusement Facilities"	0	
"Audio Streaming"	0	
Blogs	0	
"Browser Crashing Sites"	0	
"Celebrities, Entertainment"	0	
Chat	0	
"Comics, Animation"	0	
"Consumer Lending"	0	
"Coupon Sites"	0	
"Credit Cards, Online Payment, E-Money"	0	
"Crime, Weapons"	0	
--More--		

Output Parameter	Description
Category	Category names, including both provider categories and custom categories.
Custom Matches	Custom match criteria.
Category Hits	The number of times the category has been hit - that is, the number of times a website has been categorized into the category.
Custom	Indicate whether the category is custom category or not. Those that are not custom are provider categories.

Related commands

- [rule \(web-control\)](#)
- [show running-config web-control](#)
- [show web-control rules](#)
- [web-control](#)

show web-control rules

Overview Use this command to display the Web Control rules.
For more information about rules, see the [rule \(web-control\)](#) command.

Syntax `show web-control rules`

Mode Privileged Exec

Examples To show all Web Control rules, use the command:

```
awplus# show web-control rules
```

Output Figure 62-8: Example output from the **show web-control rules** command

#show web-control rules				
ID	Action	Category	From	Hits
10	deny	"Online Trading"	rd.test.qa	0
20	permit	"Browser Crashing Sites"	market.sales	1
25	permit	suspicious_sites	rd	2

Output Parameter	Description
ID	Rule ID.
Action	The action taken whenever the rule is hit.
Category	The category the rule applies to.
From	The source entity the rule applies to.
Hits	The number of times the rule has been hit.

Related commands

- [rule \(web-control\)](#)
- [show running-config web-control](#)
- [show web-control categories](#)
- [web-control](#)

web-control

Overview Use this command to enter the Web Control Configuration mode and configure Web Control functionality.

Use the **no** variant of this command to remove all configuration for Web Control. Custom categories, rules and other configuration associated with Web Control will be deleted.

Syntax `web-control`
`no web-control`

Mode Global Configuration

Usage notes This command allows you to enter the Web Control Configuration mode. This mode also contains the sub- mode of Web Control Category Configuration. For more information about the sub-mode, see the [category \(web-control\)](#) command.

The Web Control Configuration mode enables you to:

- Enable Web Control protection, see the [protect \(web-control\)](#) command.
- Configure the website categorization provider, see the [provider \(web-control\)](#) command.
- Create categories and associated match criteria, see the [category \(web-control\)](#) command.
- Create, delete and move rules for categories, see the [rule \(web-control\)](#) command and the [move rule \(web-control\)](#) command.
- Configure the default action for HTTP and HTTPS requests that do not hit any rule, see the [action \(web-control\)](#) command.

If you want to disable Web Control protection without removing the configuration, you can use the **no** variant of the [protect \(web-control\)](#) command to do so.

Examples To enter the Web Control Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# web-control
awplus(config-web-control)#
```

To destroy all Web Control configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no web-control
```

Related commands [show running-config](#)
[show running-config web-control](#)
[show web-control](#)

Command changes Version 5.4.7-1.1: HTTPS support added.

web-control categorize

Overview Use this command to inquire about which web control categories website URLs belong to.

Syntax `web-control categorize [<url-list>]`

Parameter	Description
<code><url-list></code>	One or more website HTTP or HTTPS URLs, separated by a space. If neither 'http://' nor 'https://' is specified in the URL, the default 'http://' is automatically added.

Mode Privileged Exec

Usage notes When you use this command, the device sends an inquiry to the web control provider's server. The server responds with a category for each URL.

You can use this information together with web control rules to permit or deny traffic for the particular categories.

For inquiries about HTTPS URLs, only the domain part of the URL is sent to the web control provider for categorization. This is the expected behaviour for HTTPS traffic, where only the domain name specified in TLS SNI is available for access.

Example To determine the category to which the following website URLs belong, use the command:

```
awplus# web-control categorize http://www.ebay.com  
http://www.amazon.com
```

For each URL in the inquiry, the server responds with a web control category. If it cannot categorize the URL, it displays 'unknown category'.

```
awplus#web-control categorize http://www.ebay.com http://www.amazon.com  
http://ebay.com ==> 54 (Online Auctions)  
http://www.amazon.com ==> 55 (Online Shopping)
```

Related commands [rule \(web-control\)](#)

Command changes Version 5.4.7-2.1: command added

63

Application Awareness Commands

Introduction

This chapter provides an alphabetical reference of commands used to configure application awareness, which uses Deep Packet Inspection (DPI). For more information about application awareness and a configuration example, see the [Application Awareness Feature Overview and Configuration_Guide](#).

- Command List**
- [“counters detailed”](#) on page 2687
 - [“dpi”](#) on page 2688
 - [“enable \(dpi\)”](#) on page 2689
 - [“hostname \(application\)”](#) on page 2691
 - [“provider \(dpi\)”](#) on page 2692
 - [“show dpi”](#) on page 2693
 - [“show dpi statistics”](#) on page 2695
 - [“show running-config dpi”](#) on page 2697
 - [“update-interval \(dpi\)”](#) on page 2698
 - [“web-categorization”](#) on page 2699

counters detailed

Overview Use this command to enable the display of transmit and receive counters for each entity in DPI mode.

Once you have enabled detailed counters, you can use the command **show dpi statistics <entity-name>** to display statistics for different applications on individual entities (zones, networks or hosts). This is called DPI statistics per entity.

Use the **no** variant of this command to disable DPI statistics per entity.

Syntax counters detailed
no counters detailed

Default Disabled

Mode DPI Configuration

Usage notes These counters will require system resources and should only be configured when required. Use the **no** variant to turn them off when not required.

Example To configure DPI statistics per entity, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# provider built-in
awplus(config-dpi)# enable
awplus(config-dpi)# counters detailed
```

To disable DPI statistics per entity, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# no counters detailed
```

Related commands [show dpi statistics](#)

Command changes Version 5.4.9-1.1: command added

dpi

Overview Use this command to enter DPI Configuration mode to configure DPI for application awareness.

Use the **no** variant of this command to remove all DPI configuration.

Syntax `dpi`
`no dpi`

Mode Global Configuration

Usage notes In DPI Configuration mode, you can:

- Set the DPI provider, using the [provider \(dpi\)](#) command.
- Enable DPI, using the [enable \(dpi\)](#) command.

Examples To begin configuring DPI, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)#
```

To remove all DPI configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no dpi
```

enable (dpi)

Overview Use this command to enable DPI for application awareness.

Use the **no** variant of this command to disable DPI without losing existing DPI configuration.

Syntax enable
no enable

Default DPI is disabled by default.

Mode DPI Configuration

Usage notes Use the [provider \(dpi\)](#) command to configure the DPI provider before enabling DPI.

When DPI is enabled, it can classify network traffic and identify today's most common applications.

DPI itself does not control or apply rules to the traffic. You can use the application awareness provided by DPI for:

- Network visibility
- Application Control, using the [rule \(firewall\)](#) command to enforce security policy and apply rules to the DPI applications
- Traffic Control, using the traffic control rules
- Policy-based Routing (PBR), using the PBR rules.

You can use the [show dpi statistics](#) command to show statistics for the applications being inspected by DPI.

For more information about configuring and using DPI, see the [Application Awareness Feature_Overview and Configuration Guide](#) .

Examples To enable DPI to use the built-in library, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# provider built-in
awplus(config-dpi)# enable
```

To disable DPI, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# no enable
```

**Related
commands** provider (dpi)
 show dpi
 show running-config dpi

hostname (application)

Overview Use this command to specify a hostname used by an application.

An application is a high-level definition of different types of applications being transported by network traffic. For example, social networking.

You associate a hostname or multiple hostnames with an application.

Use the **no** variant of this command to remove a hostname from an application.

Syntax `hostname <hostname>`
`no hostname`

Parameter	Description
<code><hostname></code>	The hostname expressed as a URI (Uniform Resource Identifier).

Default Not set.

Mode Application Configuration

Example To specify a hostname for the Stuff application, use the commands:

```
awplus# configure terminal
awplus(config)# application Stuff
awplus(config-application)# hostname stuff.co.nz
```

To specify an application for Youtube with multiple hostnames, use the commands:

```
awplus# configure terminal
awplus(config)# application Youtube
awplus(config-application)# hostname youtube.com
awplus(config-application)# hostnameyoutu.be
```

To remove a hostname from an application for Youtube, use the commands:

```
awplus# configure terminal
awplus(config)# application Youtube
awplus(config-application)# no hostname youtube.com
```

Related commands [application](#)

Command changes Version 5.5.2-0.1: command added

provider (dpi)

Overview Use this command to set the DPI provider for the library of applications used for DPI. Application Awareness uses DPI, if enabled, to identify applications by matching packets to a library of application signatures—either the up-to-date Procera library or the built-in library predefined in device's operating system.

Syntax `provider {procera|built-in}`

Parameter	Description
procera	Use the library provided and updated by Procera networks.
built-in	Use the library built into the device's operating system.

Default No provider is set by default.

Mode DPI Configuration

Usage notes You can use the [show application](#) command and the [show application detail](#) command to view all applications that the device recognizes. If DPI is enabled, the show commands can include the commands in the library specified with this provider command.

Note that custom applications override DPI applications, which override AlliedWare Plus predefined applications. For more information about applications, see the [application](#) command.

Note that you need to use this command before using the [enable \(dpi\)](#) command to enable DPI.

You can use the [show dpi](#) command to view the provider's current version.

Examples To set the DPI provider to the built-in library of application signatures, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# provider built-in
awplus(config-dpi)# enable
```

Related commands

- [enable \(dpi\)](#)
- [show application detail](#)
- [show dpi](#)
- [show running-config dpi](#)

Command changes Version 5.4.7-2.1: **built-in** parameter added

show dpi

Overview Use this command to show the DPI configuration state.

Syntax show dpi

Mode Privileged Exec

Examples To show information about the DPI configuration and provider's library, use the command:

```
awplus# show dpi
```

Output Figure 63-1: Example output from **show dpi** with DPI enabled and the provider set to **built-in**

```
awplus#show dpi
Status:      running
Provider:    built-in
```

Figure 63-2: Example output from **show dpi** with the provider set to **procera**, the subscription license active and DPI enabled

```
awplus#show dpi
Status:      running
Provider:    procera
Resource version:      1.0
Resource update interval: 1 hour
```

Figure 63-3: Example output from **show dpi** if the provider is set to **procera** but the subscription license is inactive

```
awplus#show dpi
Status:      unlicensed
Provider:    procera
Resource version:      not set
Resource update interval: 1 hour
```

Figure 63-4: Example output from **show dpi** with the provider built-in and web categorization provider set to **opentext**, and the subscription license active.

```
awplus#show dpi
Status:      running
Provider:    built-in
Mode:        assured
Counters:    global only
Providing application database: disabled
Web Categorization:      enabled
Web Categorization Provider: opentext
```

Table 63-1: Parameters in the output from **show dpi**

Parameter	Description
Status	The status of DPI: • running—DPI is running — DPI is enabled, and the provided library is available • disabled—DPI is disabled • unlicensed—DPI is enabled, the provider is set, but there is no valid subscription license.
Provider	The provider for the library of application signatures used to identify applications.
Resource version	The version of the library supplied by the provider, if by subscription.
Resource update interval	The interval at which a check is made for a new version of the library of application signatures, updating it if a new version is available.

Related commands [enable \(dpi\)](#)
[provider \(dpi\)](#)

show dpi statistics

Overview Use this command to display statistics for each application being inspected by DPI. This command gives you counts of the total number of packets and bytes of the applications being inspected by DPI. You can use the [rule \(firewall\)](#) command, traffic control rules or PBR rules to apply rules to the DPI applications.

You can also use this command to display application DPI statistics for an individual entity (zone, network or host). Enable this with the [counters detailed](#) command.

Syntax `show dpi statistics [<entity-name>]`

Parameter	Description
<code><entity-name></code>	The name of an individual entity, for example the name of a zone, network or host.

Mode Privileged Exec

Examples To display the statistics for each application being inspected by DPI, use the command:

```
awplus# show dpi statistics
```

Output Figure 63-5: Example output from the **show dpi statistics** command on the console.

```
awplus#show dpi statistics
```

Application	Packets	Bytes
-----	-----	-----
http	30	2020
icmp	348	29232
telnet	45	2553

To show information about the DPI statistics for an individual entity, for example the entity "joeb", use the command:

```
awplus# show dpi statistics joeb
```

Figure 63-6: Examples output from **show dpi statistics**

```
awplus#show dpi statistics joeb
```

Statistics for entity: joeb

Application	TX Packets	RX Packets	TX Bytes	RX Bytes
-----	-----	-----	-----	-----
youtube	15413	16542	15412	45123645
google	15413	654	12205	451254
facebook	4115	8153	1100	123588
twitter	15413	4865	35459	24236

Table 63-2: Parameters in the output from **show dpi statistics**

Parameter	Description
Application	The application associated with the packet
TX Packets	Transmitted packets
RX Packets	Received packets
TX Bytes	Bytes transmitted
RX Bytes	Bytes received

Related commands [counters detailed](#)

Command changes Version 5.4.7-2.1: command added
Version 5.4.9-1.1: entity parameter added

show running-config dpi

Overview Use this command to show the configuration commands that have been used to configure DPI.

Syntax `show running-config dpi`

Mode Privileged Exec

Examples To show the configuration commands that have been used to configure DPI, use the command:

```
awplus# show running-config dpi
```

Output Figure 63-7: Example output from the **show running-config dpi** command

```
awplus#show running-config dpi
dpi
  provider built-in
  enable
!
```

update-interval (dpi)

Overview Use this command to configure the update check interval for the DPI resource files if the provider is set to **procera**.

Use the **no** variant of this command to restore the default update check interval to 1 hour.

Syntax `update-interval {minutes <10-525600>|hours <1-8760>|days <1-365>|weeks <1-52>|never}`
`no update-interval`

Parameter	Description
minutes <10-525600>	Update interval from 10 through 52600 minutes
hours <1-8760>	Update interval from 1 hour through 8760 hours
days <1-365>	Update interval from 1 day through 365 days
weeks <1-52>	Update interval from 1 week through 52 weeks
never	Never update the resource.

Default The default update interval is 1 hour.

Mode DPI Mode

Usage notes The Update Manager will perform an update check for a resource when triggered by an update check interval. It will request the current version number of the resource from the Update Server, then compare it with the current local version. If they are different, the Update Manager will initiate an update of the local resource.

Note that when a feature is disabled, regular and manual update checks for its resources are disabled.

Also note that an update check for a resource will not proceed if an update of that resource is already in progress.

Examples To check and update the DPI resource files once a week, use the following command:

```
awplus(config-dpi)# update-interval weeks 1
```

To disable updating of the resource, use the following command:

```
awplus(config-dpi)# update-interval never
```

To restore the default update interval (1 hour), use the following command:

```
awplus(config-dpi)# no update-interval
```

Related Command [provider \(dpi\)](#)
[show resource](#)

web-categorization

Overview Use this command to configure DPI's web-categorization and optionally a provider. DPI's web-categorization classifies network traffic into provider defined categories (e.g. online auctions, social networking) and/or user defined custom categories.

Use Web-categorization to help protect users on the network based on the type of website they access.

Use the **no** variant of this command to disable web-categorization.

Syntax `web-categorization [digital-arts|opentext]`
`no web-categorization`

Parameter	Description
digital-arts	Use the Digital Arts provider and their database of categories.
opentext	Use the OpenText provider and their database of categories.

Default Disabled

Mode DPI Configuration

Usage notes Web-categorization requires a Web Control subscription license.

Examples To enable DPI Web-categorization and set the provider to Digital Arts, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# web-categorization digital-arts
```

To enable DPI Web-categorization and set the provider to OpenText, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# web-categorization opentext
```

To enable DPI Web-categorization with no external provider, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# web-categorization
```

To disable DPI Web-categorization, use the commands:

```
awplus# configure terminal
awplus(config)# dpi
awplus(config-dpi)# no web-categorization
```

**Related
commands**

[enable \(dpi\)](#)
[show dpi statistics](#)
[show running-config dpi](#)
[show dpi](#)

**Command
changes**

Version 5.5.3-0.1: **opentext** parameter added
Version 5.5.2-0.1: command added

64

IP Reputation Commands

Introduction

This chapter provides an alphabetical reference of commands used to configure AlliedWare Plus IP Reputation. For more information about IP Reputation and its configuration, see the IP Reputation sections contained within the [Advanced Network Protection Feature Overview and Configuration Guide](#).

The table below lists the IP Reputation commands and their applicable modes.

Figure 64-1: IP Reputation Commands and Applicable Modes

Mode	Command
Privileged Exec	<code>show ip-reputation</code>
	<code>show ip-reputation categories</code>
	<code>show running-config ip-reputation</code>
Global Configuration	<code>ip-reputation</code>
IP Reputation Mode	<code>category action (IP Reputation)</code>
	<code>protect (IP Reputation)</code>
	<code>provider proofpoint (IP Reputation)</code>
	<code>update-interval (IP Reputation)</code>

- Command List**
- “[category action \(IP Reputation\)](#)” on page 2703
 - “[ip-reputation](#)” on page 2705
 - “[protect \(IP Reputation\)](#)” on page 2706
 - “[provider proofpoint \(IP Reputation\)](#)” on page 2707
 - “[show ip-reputation](#)” on page 2708
 - “[show ip-reputation categories](#)” on page 2709

- [“show running-config ip-reputation”](#) on page 2711
- [“update-interval \(IP Reputation\)”](#) on page 2712
- [“whitelist \(IP Reputation\)”](#) on page 2714

category action (IP Reputation)

Overview Use this command to configure an action for a specified category.

Use the **no** variant of this command to set action for a specified category to default, which is alert.

Syntax `category <category-name> action {alert|deny|disable}`
`no category <category-name> action`

Parameter	Description
<category-name>	Category name. A category contains a group of IP reputation criteria that are used to classify the nature of a host reputation. A host may have a reputation in multiple categories. You can use the show ip-reputation categories command to view the categories and their status.
alert	Generate a log message. This is the default action.
deny	Drop matching packets. No error message is sent back to the source host.
disable	Ignore a specified category. Ignored categories will not be used to categorize traffic.

Default The default action is alert.

Mode IP Reputation Mode

Usage notes You can only configure the categories from the IP Reputation database provider, which is Proofpoint. You can use the [show ip-reputation categories](#) command to see the list of IP Reputation categories.

NOTE: Note that you should use the [provider proofpoint \(IP Reputation\)](#) command to configure the provider before configuring the action.

Examples To drop packets categorized as P2P, use the commands:

```
awplus# configure terminal
awplus(config)# ip-reputation
awplus(config-ip-reputation)# provider proofpoint
awplus(config-ip-reputation)# category P2P action deny
```

To set the action for category P2P to default, use the commands:

```
awplus# configure terminal
awplus(config)# ip-reputation
awplus(config-ip-reputation)# no category P2P action
```

**Related
commands** `show ip-reputation categories`
 `show running-config ip-reputation`

ip-reputation

Overview Use this command to configure IP Reputation.

Use the **no** variant of this command to remove all IP Reputation configuration.

Syntax `ip-reputation`
`no ip-reputation`

Mode Global Configuration

Usage notes This command allows you to enter the IP Reputation mode. The command prompt for this mode is **awplus(config-ip-reputation)#**.

In the IP Reputation mode, you can:

- Set or remove the IP Reputation database provider, see the [provider proofpoint \(IP Reputation\)](#) command.
- Enable or disable IP Reputation protection, see the [protect \(IP Reputation\)](#) command.
- Configure the action for specified categories, see the [category action \(IP Reputation\)](#) command.

Examples To configure IP Reputation, use the commands:

```
awplus# configure terminal
awplus(config)# ip-reputation
awplus(config-ip-reputation)#
```

To remove all IP Reputation configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no ip-reputation
```

Related commands [show ip-reputation](#)
[show running-config ip-reputation](#)

protect (IP Reputation)

Overview Use this command to enable IP Reputation protection.

Use the **no** variant of this command to disable IP Reputation protection without losing existing configuration.

Once IP Reputation protection is enabled, traffic will be categorized according to the available IP Reputation categories. See the [show ip-reputation categories](#) command for the list of available IP Reputation categories.

Note that you should use the [provider proofpoint \(IP Reputation\)](#) command to set the IP Reputation database provider before issuing this command.

Syntax protect
no protect

Default IP Reputation protection is disabled by default.

Mode IP Reputation Mode

Examples To enable IP Reputation protection, use the commands:

```
awplus# configure terminal
awplus(config)# ip-reputation
awplus(config-ip-reputation)# provider proofpoint
awplus(config-ip-reputation)# protect
```

To disable IP Reputation protection, use the commands:

```
awplus# configure terminal
awplus(config)# ip-reputation
awplus(config-ip-reputation)# no protect
```

Related commands [show ip-reputation](#)
[show running-config ip-reputation](#)

provider proofpoint (IP Reputation)

Overview Use this command to set the IP Reputation database provider.

Proofpoint provides a database of IP reputation based on threat analysis. The database is regularly updated and can deliver the latest information of identified and potentially harmful IP addresses classified in categories.

If the provider is configured, you can use the [show ip-reputation categories](#) command to show the category details from the provider.

The default action for all categories is alert and you can use the [category action \(IP Reputation\)](#) command to set the action for a specified category.

Syntax `provider proofpoint`

Mode IP Reputation Mode

Examples To set the IP Reputation database provider, use the commands:

```
awplus# configure terminal
awplus(config)# ip-reputation
awplus(config-ip-reputation)# provider proofpoint
```

Related commands [show ip-reputation](#)
[show running-config ip-reputation](#)
[show ip-reputation categories](#)

show ip-reputation

Overview Use this command to show the IP Reputation configuration state, including the IP Reputation database provider.

Syntax `show ip-reputation`

Mode Privileged Exec

Examples To show the IP Reputation configuration state, use the command:

```
awplus# show ip-reputation
```

Output Figure 64-2: Example output from **show ip-reputation** if the IP Reputation subscription license is active.

```
awplus#show ip-reputation
Status:      Enabled (Active)
Events:      23
Provider:    Proofpoint
  Resource version: 1.0
  Entry count:    148357
  Status:         Enabled
  Resource update interval: 1 hour
```

Related commands [ip-reputation](#)

Command changes Version 5.4.7-0.1: Event count added to the command output.

show ip-reputation categories

Overview Use this command to show the IP Reputation category details.

Note that you need to use the [provider proofpoint \(IP Reputation\)](#) command to set the IP Reputation database provider before issuing this command.

Syntax `show ip-reputation categories`

Mode Privileged Exec

Examples To show the IP Reputation category details, use the command:

```
awplus# show ip-reputation categories
```

Output Figure 64-3: Example output from the **show ip-reputation categories** command

```
awplus#show ip-reputation categories
```

Category(* = invalid)	Action	Description
AbusedTLD	alert	Abused or free TLD Related
Bitcoin_Related	alert	Bitcoin Mining and related
Blackhole	alert	Blackhole or Sinkhole systems
Bot	alert	Known Infected Bot
Brute_Forcer	alert	SSH or other brute forcer
ChatServer	alert	POLICY Chat Server
CnC	alert	Malware Command and Control Server
Compromised	alert	Known compromised or Hostile
DDoSAttacker	alert	DDoS Source
DriveBySrc	alert	Driveby Source
Drop	alert	Drop site for logs or stolen credentials
DynDNS	alert	Domain or IP Related to a Dynamic DNS Entry or Request
EXE_Source	alert	Suspicious exe or dropper service
FakeAV	alert	Fake AV and AS Products
IPCheck	alert	IP Check Services
Mobile_CnC	alert	Known CnC for Mobile specific Family
Mobile_Spyware_CnC	alert	Spyware CnC specific to mobile devices
OnlineGaming	alert	Questionable Gaming Site
P2P	alert	P2P Node
P2PCnC	alert	Distributed CnC Nodes
Parking	alert	Domain or SEO Parked
RemoteAccessService	alert	GoToMyPC and similar remote access services
Scanner	alert	Host Performing Scanning
Skype_SuperNode	alert	Observed Skype Bootstrap or Supernode
Spam	alert	Known Spam Source
SpywareCNS	alert	Spyware Reporting Server
TorNode	alert	POLICY Tor Node
Undesirable	alert	Undesirable but not illegal
Utility	alert	Known Good Public Utility
VPN	alert	VPN Server

**Related
commands** [category action \(IP Reputation\)](#)

show running-config ip-reputation

Overview Use this command to show the configuration commands that have been used to configure IP Reputation.

Syntax `show running-config ip-reputation`

Mode Privileged Exec

Examples To show the commands that have been used to configure IP Reputation, use the command:

```
awplus# show running-config ip-reputation
```

Output Figure 64-4: Example output from **show running-config ip-reputation**

```
awplus#show running-config ip-reputation
ip-reputation
  category Scanner action deny
  provider proofpoint
  whitelist 192.0.2.5
  protect
!
```

Related commands

- [ip-reputation](#)
- [show ip-reputation](#)
- [whitelist \(IP Reputation\)](#)

update-interval (IP Reputation)

Overview Use this command to configure an update check interval for the IP Reputation resource files.

Use the **no** variant of this command to restore the default update check interval to 1 hour.

Syntax `update-interval {minutes <10-525600>|hours <1-8760>|days <1-365>|weeks <1-52>|never}`

`no update-interval`

Parameter	Description
minutes <10-525600>	Update interval from 10 through 52600 minutes
hours <1-8760>	Update interval from 1 hour through 8760 hours
days <1-365>	Update interval from 1 day through 365 days
weeks <1-52>	Update interval from 1 week through 52 weeks
never	Never update the resource. If IP Reputation becomes enabled, the Update Manager will do update check and update the resource files if needed. Use the protect (IP Reputation) command to enable IP Reputation.

Default The default update interval is 1 hour.

Mode IP Reputation Mode

Usage notes The Update Manager will perform an update check for a resource when triggered by an update check interval. It will request the current version number of the resource from the Update Server, then compare it with the current local version. If they are different, the Update Manager will initiate an update of the local resource.

Note that when a feature is disabled, regular and manual update checks for its resources are disabled.

Also note that an update check for a resource will not proceed if an update of that resource is already in progress.

Examples To check and update the IP Reputation resource files once a week, use the following command:

```
awplus(config-ip-reputation)# update-interval weeks 1
```

To disable updating of the resource, use the following command:

```
awplus(config-ip-reputation)# update-interval never
```

To restore the default update interval, which is 1 hour, use the following command:

```
awplus(config-ip-reputation)# no update-interval
```

Related [show resource](#)
commands

whitelist (IP Reputation)

Overview Use this command to add an IP address to the IP Reputation whitelist.
Use the **no** variant of this command to remove an IP address from the whitelist.

Syntax `whitelist <ip-address>`
`no whitelist <ip-address>`

Parameter	Description
<code><ip-address></code>	The IPv4 address to add to or remove from the IP reputation whitelist, in dotted-decimal format.

Default There are no IP addresses in the IP reputation whitelist by default.

Mode IP Reputation Configuration

Usage notes If an IP address has acquired a bad reputation but, in spite of the risk, you still wish to be able to send traffic to or receive traffic from that address without it being alerted or denied, you can add that address to the IP Reputation whitelist. Use this **whitelist** command.

When the address no longer needs to be in the whitelist, we recommend removing it. Use the **no** variant of this command.

Example To add IP address 192.0.2.5 to the IP reputation whitelist, use the commands:

```
awplus# configure terminal
awplus(config)# ip-reputation
awplus(config-ip-reputation)# whitelist 192.0.2.5
```

Related commands [ip-reputation](#)
[show running-config ip-reputation](#)

Command changes Version 5.4.9-2.1: command added

Part 10: Virtual Private Networks (VPNs)

65

IPsec Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Internet Protocol Security (IPsec) tunnel.

For introductory information about IPsec tunnel in AlliedWare Plus, including overview and configuration information, see the:

- [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#)
- [GRE and Multipoint VPNs Feature Overview and Configuration Guide](#)

- Command List**
- [“clear isakmp sa”](#) on page 2718
 - [“crypto ipsec profile”](#) on page 2719
 - [“crypto isakmp key”](#) on page 2721
 - [“crypto isakmp peer”](#) on page 2724
 - [“crypto isakmp profile”](#) on page 2726
 - [“debug isakmp”](#) on page 2728
 - [“dpd-interval”](#) on page 2730
 - [“dpd-timeout”](#) on page 2731
 - [“interface tunnel \(IPsec\)”](#) on page 2732
 - [“lifetime \(IPsec Profile\)”](#) on page 2733
 - [“lifetime \(ISAKMP Profile\)”](#) on page 2734
 - [“no debug isakmp”](#) on page 2735
 - [“pfs”](#) on page 2736
 - [“rekey”](#) on page 2738
 - [“show debugging isakmp”](#) on page 2739
 - [“show interface tunnel \(IPsec\)”](#) on page 2740

- [“show ipsec counters”](#) on page 2742
- [“show ipsec peer”](#) on page 2743
- [“show ipsec policy”](#) on page 2744
- [“show ipsec profile”](#) on page 2745
- [“show ipsec sa”](#) on page 2747
- [“show isakmp counters”](#) on page 2748
- [“show isakmp key \(IPsec\)”](#) on page 2749
- [“show isakmp peer”](#) on page 2750
- [“show isakmp profile”](#) on page 2751
- [“show isakmp sa”](#) on page 2753
- [“show tunnel inline-processing counters”](#) on page 2754
- [“transform \(IPsec Profile\)”](#) on page 2756
- [“transform \(ISAKMP Profile\)”](#) on page 2758
- [“tunnel destination \(IPsec\)”](#) on page 2760
- [“tunnel inline-processing”](#) on page 2762
- [“tunnel local name \(IPsec\)”](#) on page 2763
- [“tunnel local selector”](#) on page 2764
- [“tunnel mode ipsec”](#) on page 2766
- [“tunnel oper-status-control”](#) on page 2767
- [“tunnel protection ipsec \(IPsec\)”](#) on page 2770
- [“tunnel remote name \(IPsec\)”](#) on page 2771
- [“tunnel remote selector”](#) on page 2772
- [“tunnel security-reprocessing”](#) on page 2774
- [“tunnel selector paired”](#) on page 2775
- [“tunnel source \(IPsec\)”](#) on page 2776
- [“undebg isakmp”](#) on page 2778
- [“version \(ISAKMP\)”](#) on page 2779

clear isakmp sa

Overview Use this command to delete Internet Security Association Key Management Protocol (ISAKMP) Security Associations (SAs). SAs specify the Security Parameter Index (SPI), protocols, algorithms and keys for protecting a single flow of traffic between two IPsec peers. For more information about SA, see the [Internet Protocol Security \(IPSec\) Feature Overview and Configuration Guide](#).

Syntax `clear [crypto] isakmp sa [peer <ipv4-addr>|<ipv6-addr>|<hostname>] [force]`

Parameter	Description
<ipv4-addr>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	Destination IPv6 address. The IPv4 address uses the format X:X::X:X.
<hostname>	Destination host name.
force	Force to clear ISAKMP SAs without negotiating with the peer.

Mode Privileged Exec

Examples To delete the ISAKMP security associations at the peer for an IPv6 address, use the command:

```
awplus# clear isakmp sa peer 2001:0db8::1
```

To delete the ISAKMP security associations at the peer for an IPv4 address, use the command:

```
awplus# clear isakmp sa peer 192.168.2.1
```

To delete the ISAKMP security associations at the peer for a host name, use the command:

```
awplus# clear isakmp sa peer remote.example.com
```

Related commands [crypto isakmp key](#)
[show isakmp sa](#)

Command Changes Version 5.4.7-0.1: Parameter <hostname> added for DDNS feature.

crypto ipsec profile

Overview Use this command to configure a custom IPsec profile.

An IPsec profile comprises one or more transforms that can be configured by using the [transform \(IPsec Profile\)](#) command.

Use the **no** variant to delete a previously created profile.

Syntax `crypto ipsec profile <profile_name>`
`no crypto ipsec profile <profile_name>`

Parameter	Description
<profile_name>	Profile name. Profile names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Profile names can have only letters from a to z and A to Z, numbers from 0 to 9, - (dash), or _ (underscore).

Default The default IPsec profile with transforms in order of preference is listed in the following table. Which IPsec profile will actually be used depends on how the negotiation between the peers is carried out when establishing the connection. Note that you cannot delete or edit the default profile. Expiry time of 8 hours applies to the default IPsec profile.

Table 65-1: IPsec default profile

Attribute	Transform 1	Transform 2	Transform 3	Transform 4	Transform 5	Transform 6
Protocol	ESP	ESP	ESP	ESP	ESP	ESP
Encryption (all CBC)	AES256	AES256	AES128	AES128	3DES	3DES
Integrity (all HMAC)	SHA256	SHA1	SHA256	SHA1	SHA256	SHA1

Mode Global Configuration

Examples To configure a custom IPsec profile for establishing IPsec SAs with a remote peer, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# transform 2 protocol esp
integrity sha1 encryption 3des
```

To delete a custom profile, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto ipsec profile my_profile
```

**Related
commands**

- lifetime (IPsec Profile)
- show ipsec profile
- transform (IPsec Profile)

crypto isakmp key

Overview Use this command to configure an ISAKMP authentication key. These keys can be of type Pre-shared Key (PSK) or Extensible Authentication Protocol (EAP). Keys are stored encrypted in the running-configuration.

You must configure this key whenever you specify authentication keys in an (Internet Key Exchange) IKE policy and at both peers.

This command specifies both the value of the key and also an identifier (the hostname, address or policy parameters). This identifier is used to decide which key to use for a particular ISAKMP message exchange.

See the Usage section below for more information, and see the following guides for examples:

- [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#)
- [GRE and Multipoint VPNs Feature Overview and Configuration Guide](#)

Use the **no** variant to remove a key.

Syntax

```
crypto isakmp key [8] <key> hostname <hostname> [type {eap|psk}]
no crypto isakmp key [8] <key> hostname <hostname> [type {eap|psk}]

crypto isakmp key [8] <key> address {<ipv4-addr>|<ipv6-addr>} [type {eap|psk}]
no crypto isakmp key [8] <key> address {<ipv4-addr>|<ipv6-addr>} [type {eap|psk}]

crypto isakmp key [8] <key> policy <policy-name> [type {eap|psk}]
no crypto isakmp key [8] <key> policy <policy-name> [type {eap|psk}]
```

Parameter	Description
crypto	Security specific command.
isakmp	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
key	Pre-shared key (PSK) or Extensible Authentication Protocol (EAP).
<key>	Specify the key. Use any combination of alphanumeric characters up to 128 bytes.
8	Specifies that an encrypted key follows.
<hostname>	A hostname (e.g. example.com).
<ipv4-addr>	IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	IPv6 address. The IPv6 address uses the format X:X::X:X.

Parameter	Description
<code><policy-name></code>	The local policy name. This is the name of the tunnel (e.g. tunnel2).
<code>type</code>	ISAKMP key type
<code>eap</code>	Extensible Authentication Protocol. This can be used with multipoint VPN when performing RADIUS authentication. See the GRE and Multipoint VPNs Feature Overview and Configuration Guide for more information.
<code>psk</code>	Pre-shared Key (default)

Default ISAKMP keys do not exist.

Mode Global Configuration

Usage notes Use this command to configure an authentication key for use with the ISAKMP protocol.

Before a tunnel can be protected by IPsec, each endpoint of the tunnel must verify that they are communicating with an authorized entity. ISAKMP uses authentication keys in the initial handshake between peers to ensure both endpoints are allowed to communicate.

This command specifies both the value of the key and also an identifier which is used to decide which key to use for a particular ISAKMP message exchange. Because the responding endpoint does not identify itself to the local device until after the key is used, it is important that the key identifier is part of the tunnel configuration on the initiating device.

The tunnel configuration parameter used to select which key to use when negotiating IPsec protection for that tunnel is in priority order:

- 1) **tunnel remote name**
- 2) **tunnel destination <ipv4-address>|<ipv6-address>** (if the remote name is not specified)
- 3) **tunnel local name**
- 4) **tunnel source <ipv4-address>|<ipv6-address>** (if the remote name is not specified)

For point-to-point tunnels, we recommend you configure local and remote names on the tunnels. Then use the remote name of the other device to identify the authentication keys on the local device.

For point-to-multipoint tunnels, it may be necessary to identify the authentication key by the local name of the tunnel, if the ISAKMP negotiation is to be initiated by that tunnel. This is because it is not possible to configure multiple remote names. However, it is possible to use the expected remote addresses or names of the remote initiating tunnels to identify keys. This is because the remote tunnel will identify itself when it initiates a connection.

Examples To configure a pre-shared authentication key of “friend”, using a hostname, use the commands below:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend hostname
mypeer@my.domain.com
```

To remove that pre-shared key, use the commands below:

```
awplus# configure terminal
awplus(config)# no crypto isakmp key friend hostname
mypeer@my.domain.com
```

To configure a pre-shared already-encrypted authentication key, using an IPv4 address, use the commands below:

```
awplus# configure terminal
awplus(config)# crypto isakmp key 8 Nhe6ioQmzbysQaJr6Du+cA==
address 192.168.1.2
```

To configure a pre-shared key, using the local policy “tunnel2”, use the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend policy tunnel2
```

To remove that key, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp key friend policy tunnel2
```

To configure an ISAKMP key using EAP, enter the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend hostname example.com
type eap
```

Related commands

- [show isakmp key \(IPsec\)](#)
- [tunnel destination \(IPsec\)](#)
- [tunnel local name \(IPsec\)](#)
- [tunnel remote name \(IPsec\)](#)

Command changes

- Version 5.4.9-0.1: **type** parameter added
- Version 5.4.9-1.1: **policy** parameter added

crypto isakmp peer

Overview Use this command to configure a peer to use a specific ISAKMP profile.

Use the **no** variant to set the peer back to using the default profile.

Syntax

```
crypto isakmp peer address {<ipv4-addr>|<ipv6-addr>} profile <profile-name>
no crypto isakmp peer address {<ipv4-addr>|<ipv6-addr>} profile
crypto isakmp peer dynamic profile <profile-name>
no crypto isakmp peer dynamic profile
crypto isakmp peer hostname <hostname> profile <profile-name>
no crypto isakmp peer hostname <hostname> profile
crypto isakmp peer policy <policy-name> profile <profile-name>
no crypto isakmp peer policy <policy-name> profile
```

Parameter	Description
<ipv4-addr>	IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	IPv6 address. The IPv6 address uses the format X:X::X:X.
dynamic	Remote endpoint with a dynamic IP address.
<hostname>	Remote endpoint with a host name as the destination.
<policy-name>	The name of a local policy. This is the name of the tunnel (e.g. tunnel2).
<profile-name>	Profile name.

Default By default, all peers use the default profile.

Mode Global Configuration

Usage notes Use this command to configure a peer to use a specific ISAKMP profile.

When IPsec protection is applied to a tunnel, an ISAKMP profile is selected for use when IPsec parameters need to be negotiated. This profile is chosen when the tunnel first becomes active, and so must be selected based on local configuration only.

The tunnel configuration parameter used to select which ISAKMP profile to use when negotiating IPsec protection for that tunnel is in the following priority order:

- 1) **tunnel destination dynamic** (if a dynamic profile has been configured)
- 2) **tunnel endpoint dynamic** (if a dynamic profile has been configured)
- 3) **tunnel remote name**

- 4) **tunnel destination** <ipv4-address>|<ipv6-address> (if the remote name is not specified)
- 5) **tunnel endpoint** <ipv4-address>
- 6) **tunnel local name**
- 7) **tunnel source** <ipv4-address>|<ipv6-address> (if the remote name is not specified)
- 8) **tunnel destination** <hostname> (if the hostname is not specified)
- 9) **tunnel endpoint** <hostname> (if the hostname is not specified)

Examples To configure a profile for a peer, using a dynamic IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp peer dynamic profile peer_profile
```

To set the profile for the peer back to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp peer dynamic profile
```

To configure a profile for a peer, using a local policy name of "tunnel2", use the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp peer policy tunnel2 profile
peer-profile
```

To set the profile for the peer back to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp peer policy tunnel2 profile
```

Related commands

- [show isakmp peer](#)
- [tunnel destination \(IPsec\)](#)
- [tunnel endpoint](#)
- [tunnel local name \(IPsec\)](#)
- [tunnel source \(IPsec\)](#)
- [tunnel remote name \(IPsec\)](#)

Command Changes

- Version 5.4.7-0.1: **hostname** parameter added.
- Version 5.4.9-1.1: **policy** parameter added.

crypto isakmp profile

Overview Use this command to configure a custom ISAKMP profile.

An ISAKMP profile comprises one or more transforms that can be configured by using the [transform \(ISAKMP Profile\)](#) command.

Use the **no** variant to delete a previously created profile.

Syntax `crypto isakmp profile <profile_name>`
`no crypto isakmp profile <profile_name>`

Parameter	Description
<code><profile_name></code>	Profile name. Profile names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Profile names can have only letters from a to z and A to Z, numbers from 0 to 9, - (dash), or _ (underscore).

Default Which ISAKMP profile transform will actually be used depends on how the negotiation between the peers is carried out when establishing the connection. For more information about default ISAKMP profiles, see the following table. Note that you cannot delete or edit the default profile. Expiry time of 24 hours applies to the default profile.

Table 65-2: ISAKMP default profile

Attribute	Encryption	Integrity	Group	Authentication
Transform 1	AES256	SHA256	14	Pre-shared
Transform 2	AES256	SHA256	16	Pre-shared
Transform 3	AES256	SHA1	14	Pre-shared
Transform 4	AES256	SHA1	16	Pre-shared
Transform 5	AES128	SHA256	14	Pre-shared
Transform 6	AES128	SHA256	16	Pre-shared
Transform 7	AES128	SHA1	14	Pre-shared
Transform 8	AES128	SHA1	16	Pre-shared
Transform 9	3DES	SHA256	14	Pre-shared
Transform 10	3DES	SHA256	16	Pre-shared
Transform 11	3DES	SHA1	14	Pre-shared
Transform 12	3DES	SHA1	16	Pre-shared

Mode Global Configuration

Examples To configure a custom ISAKMP profile for establishing ISAKMP SAs with a remote peer, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# transform 2 integrity sha1
encryption 3des group 5
```

To delete a custom profile, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp profile my_profile
```

Related commands

- [dpd-interval](#)
- [dpd-timeout](#)
- [lifetime \(ISAKMP Profile\)](#)
- [transform \(ISAKMP Profile\)](#)
- [version \(ISAKMP\)](#)

Validation Commands

- [show isakmp profile](#)

debug isakmp

Overview Use this command to enable debugging ISAKMP.
To disable debugging ISAKMP, see [no debug isakmp](#) or [undebug isakmp](#).

Syntax debug [crypto] isakmp [info|trace|all]

Parameter	Description
debug	Debugging function.
crypto	Security specific command.
isakmp	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
info	Informational debug messages such as protocol events.
trace	Verbose debug messages including protocol events and message traces.
all	All debug enabled.

Mode Privileged Exec

Examples Figure 65-1: Example output from the **debug isakmp** command on the console.

```
awplus#debug isakmp info
awplus#terminal monitor
% Warning: Console logging enabled
awplus#show ipsec peer
21:03:42 awplus IMISH[30349]: show ipsec peer

10.2.0.10
  IPSEC
    Selector: 0.0.0.0/0 0.0.0.0/0    tunnel1
    Profile: default
  ISAKMP
    LocalID: 10.1.0.10
    RemoteID: 10.2.0.10
awplus#ping 192.168.1.2

PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
21:04:13 awplus iked: [DEBUG]: ike_pfkey.c:622:sadb_acquire_callback():
sadb_acquire_callback: seq=6 reqid=409
6 satype=96 sa_src=10.1.0.10[0] sa_dst=10.2.0.10[0] samode=229 selid=1
21:04:13 awplus iked: [DEBUG]: isakmp.c:918:isakmp_initiate(): new request (seq:6
spid:1 reqid:4096)
21:04:13 awplus iked: [DEBUG]: ikev2.c:758:ikev2_initiate(): creating new ike_sa
21:04:13 awplus iked: [DEBUG]: ike_sa.c:431:ikev2_allocate_sa():
ikev2_create_sa(nil), 10.1.0.10[500], 10.2.0
.10[500], 0x810b678)
21:04:13 awplus iked: [DEBUG]: ike_sa.c:434:ikev2_allocate_sa(): sa: 0x810d3a0
21:04:13 awplus iked: [DEBUG]: ikev2.c:800:ikev2_initiate(): child_sa: 0x810dd60
21:04:13 awplus iked: [DEBUG]: ikev2_child.c:139:ikev2_child_state_set(): child_sa
0x810dd60 state IDLING -> G
ETSPI
21:04:13 awplus iked: [DEBUG]: ike_pfkey.c:269:sadb_getspi(): sadb_getspi: seq=6,
satype=96
21:04:13 awplus iked: [DEBUG]: ike_pfkey.c:622:sadb_acquire_callback():
sadb_acquire_callback: seq=7 reqid=409
6 satype=96 sa_src=10.1.0.10[0] sa_dst=10.2.0.10[0] samode=229 selid=1
21:04:13 awplus iked: [DEBUG]: isakmp.c:918:isakmp_initiate(): new request (seq:7
spid:1 reqid:4096)
21:04:13 awplus iked: [DEBUG]: ikev2.c:800:ikev2_initiate(): child_sa: 0x810ec68
21:04:13 awplus iked: [DEBUG]: ikev2_child.c:139:ikev2_child_state_set(): child_sa
0x810ec68 state IDLING -> G
ETSPI

awplus#no debug isakmp
awplus#show debugging isakmp

ISAKMP Debugging status:
  ISAKMP Informational debugging is disabled
  ISAKMP Trace debugging is disabled
```

Related commands [no debug isakmp](#)
[undebug isakmp](#)

dpd-interval

Overview Use this command to specify the Dead Peer Detection (DPD) interval for an ISAKMP profile.

DPD is an IKE mechanism using a form of keep-alive to determine if a tunnel peer is still active.

The interval parameter specifies the amount of time the device waits for traffic from its peer before sending a DPD acknowledgment message.

Use the **no** variant to set the interval to its default (30 seconds).

Syntax `dpd-interval <10-86400>`
`no dpd-interval`

Parameter	Description
<code><10-86400></code>	Interval expressed in seconds.

Default If you do not specify an interval, the default interval of 30 seconds applies.

Mode ISAKMP Profile Configuration

Examples To specify a DPD interval, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# dpd-interval 20
```

To set the interval to its default, use the following commands:

```
awplus(config-isakmp-profile)# no dpd-interval
```

Related commands [crypto isakmp profile](#)

Validation Commands [show isakmp profile](#)

dpd-timeout

- Overview** Use this command to specify a Dead Peer Detection (DPD) timeout for IKEv1.
- DPD is an IKE mechanism using a form of keep-alive to determine if a tunnel peer is still active.
- DPD timeout defines the timeout interval after which all connections to a peer are deleted in case of inactivity. This only applies to IKEv1, in IKEv2 the default retransmission timeout applies as every exchange is used to detect dead peers.
- Use the **no** variant to set the timeout to its default (150 seconds).

- Syntax** `dpd-timeout <10-86400>`
`no dpd-timeout`

Parameter	Description
<code><10-86400></code>	Timeout in seconds.

- Default** If you do not specify a timeout, the default timeout of 150 seconds applies.

- Mode** ISAKMP Profile Configuration

- Examples** To specify a DPD timeout for IKEv1, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# dpd-timeout 200
```

To set the timeout to its default, use the following command:

```
awplus(config-isakmp-profile)# no dpd-timeout
```

- Related commands** [crypto isakmp profile](#)

- Related commands** [show isakmp profile](#)

interface tunnel (IPsec)

Overview Use this command to create a tunnel interface or to enter Interface mode to configure an existing tunnel. Tunnel interfaces are identified by an index identifier that is an integer in the range from 0 through 65535.

Use the **no** variant of this command to remove a previously created tunnel interface.

Syntax `interface tunnel<0-65535>`
`no interface tunnel<tunnel-index>`

Parameter	Description
<0-65535>	Specify a tunnel interface index identifier in the range from 0 to 65535.

Default Tunnel interfaces do not exist.

Mode Global Configuration

Usage notes After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

Note that you need to designate a tunnel mode, tunnel source address, tunnel destination address, IP address of tunnel interface and use [tunnel protection ipsec \(IPsec\)](#) command to encrypt and authenticate the packets travelling though the tunnel.

Examples To configure an IPsec tunnel interface with index 100, enter the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel100
awplus(config-if)# tunnel mode ipsec ipv4
```

To remove the IPsec tunnel interface tunnel100, enter the commands below:

```
awplus# configure terminal
awplus(config)# no interface tunnel100
```

Command changes Version 5.4.7-2.1: increased range for **tunnel** index identifier.

lifetime (IPsec Profile)

Overview Use this command to specify a lifetime for an IPsec SA.

Lifetime measures how long the IPsec SA can be maintained before it expires. Lifetime prevents a connection from being used too long.

Use the **no** variant to set the lifetime to default (28800 seconds).

Syntax `lifetime seconds <300-31449600>`
`no lifetime seconds`

Parameter	Description
<code><300-31449600></code>	Lifetime in seconds.

Default If you do not specify a lifetime, the default lifetime of 28800 seconds (8 hours) applies.

Mode IPsec Profile Configuration

Examples To specify a lifetime for an IPsec SA, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# lifetime seconds 400
```

To set the lifetime to its default, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# no lifetime seconds
```

Related commands [crypto ipsec profile](#)

lifetime (ISAKMP Profile)

Overview Use this command to specify a lifetime for an ISAKMP SA.

Lifetime measures how long the ISAKMP SA can be maintained before it expires. Lifetime prevents a connection from being used too long.

Use the **no** variant to set the lifetime to default (86400 seconds).

Syntax `lifetime <600-31449600>`
`no lifetime`

Parameter	Description
<code><600-31449600></code>	Lifetime in seconds.

Default If you do not specify a lifetime, the default lifetime of 86400 seconds (8 hours) applies.

Mode ISAKMP Profile Configuration

Examples To specify a lifetime for an ISAKMP SA, use the following commands:

```
awplus(config)# configure isakmp profile my_profile
awplus(config-isakmp-profile)# lifetime 700
```

To set the lifetime to its default, use the following commands:

```
awplus(config-isakmp-profile)# no lifetime
```

Related commands [crypto isakmp profile](#)

no debug isakmp

Overview Use this command to disable debugging ISAKMP.

To enable debugging ISAKMP, see [debug isakmp](#).

Syntax no [crypto] isakmp [info|trace|all]

Parameter	Description
no	Disable debugging function.
crypto	Security specific.
isakmp	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
info	Informational debug messages such as protocol events.
trace	Verbose debug messages including protocol events and message traces.
all	All debug enabled.

Mode Privileged Exec

Related commands [debug isakmp](#)
[undebug isakmp](#)

pfs

Overview Use this command to enable PFS and set a Diffie-Hellman group for PFS in an IPsec profile.

Use the **no** variant to disable PFS.

Syntax `pfs {2|5|14|15|16|18}`
`no pfs`

Parameter	Description
2	1024-bit MODP Group
5	1536-bit MODP Group
14	2048-bit MODP Group
15	3072-bit MODP Group
16	4096-bit MODP Group
18	8192-bit MODP Group

Default PFS is disabled.

Mode IPsec Profile Configuration

Usage notes Perfect Forward Secrecy (PFS) ensures generated keys, for example IPsec SA keys are not compromised if any other keys, for example, ISAKMP SA keys are compromised.

The specified PFS group must match the PFS group setting on the peer - especially when IKEv2 is used for ISAKMP SA negotiation. With IKEv2, if there is a PFS group mismatch an IPsec SA will be established and the tunnel will come up because PFS is not required for the initial child SA negotiation. However, when the IPsec SA rekeys it will fail due to the PFS group mismatch, and upon IPsec SA expiry the tunnel will no longer be able to carry traffic.

Examples To enable PFS and set a Diffie-Hellman group for PFS, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# pfs 15
```

To disable PFS, use the following command:

```
awplus(config-ipsec-profile)# no pfs
```

Related commands [crypto ipsec profile](#)

Validation show ipsec profile
Commands

rekey

Overview Use this command to set the rekey policy for an IPsec profile. This policy will be used to make a decision or whether the SA will rekey at its expiry.

The options are **always**, **never**, and **on-demand**. The **on-demand** option makes its decision based on whether the link has seen any traffic since the SA's last rekey.

Use the **no** variant of this command to set the rekey policy back to its default of **always**.

Syntax `rekey {always|never|on-demand}`
`no rekey`

Parameter	Description
<code>always</code>	Always rekey this SA (default)
<code>never</code>	Never rekey this SA
<code>on-demand</code>	Only rekey this SA if it has been used since the last rekey

Default By default, an IPsec SA will always rekey.

Mode IPsec Profile Configuration

Usage notes These options may be useful if you have a hub and spoke VPN topology and need to provision more than the maximum number of concurrent active VPNs supported by your device. **Never** and **on-demand** allow unused VPNs to be aged out, making more efficient use of the number of available VPNs.

Example To only rekey when traffic is detected over the interface, for the profile named 'myprofile', use the commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile myprofile
awplus(config-ipsec-profile)# rekey on-demand
```

To reset the rekey policy back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile myprofile
awplus(config-ipsec-profile)# no rekey
```

Related commands [crypto ipsec profile](#)
[show ipsec profile](#)

Command changes Version 5.4.9-2.1: command added

show debugging isakmp

Overview Use this command to show if debugging ISAKMP is enabled.

Syntax show debugging [crypto] isakmp

Parameter	Description
debugging	Debugging information.
crypto	Security specific command.
isakmp	Internet Security Association Key Management Protocol provides a common framework for key management implementations.

Mode Privileged Exec

Examples To show if debugging ISAKMP is enabled, enter the command below:

```
awplus# show debugging isakmp
```

Output Figure 65-2: Example output from the **show debugging isakmp** command

```
awplus#show debugging isakmp
ISAKMP Debugging status:
  ISAKMP Informational debugging is enabled
  ISAKMP Trace debugging is disabled
```

show interface tunnel (IPsec)

Overview Use this command to display status information of tunnels.

The tunnel remains inactive if no valid tunnel source or tunnel destination is configured.

Syntax `show interface tunnel< tunnel-index>`

Parameter	Description
tunnel	Specify this parameter to display tunnel status information of a given tunnel identified by the < tunnel-index> parameter.
< tunnel-index>	Specify a tunnel index in the range from 0 through 65535.

Mode Privileged Exec

Examples To display status information for IPsec tunnel 'tunnel2', use the command:

```
awplus# show interface tunnel2
```

Output Figure 65-3: Example output from the **show interface tunnel** command

```
awplus#show interface tunnel2
Interface tunnel2
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 192.168.1.2/30
  index 23 metric 1 mtu 1438
  <UP,RUNNING,MULTICAST>
  VRF Binding: Not bound
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Tunnel source eth1 (200.1.45.1), destination 200.1.15.1
  Tunnel name local 200.1.45.1, remote 200.1.15.1
  Tunnel traffic selectors (ID, local, remote)
    1    0.0.0.0/0          0.0.0.0/0
  Tunnel protocol/transport ipsec ipv4, key disabled, sequencing disabled
  Checksumming of packets disabled, DF bit set, path MTU discovery disabled
  Tunnel protection via IPsec (profile "default")
  Tunnel inline-processing enabled
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0, broadcast packets 0
    input average rate : 30 seconds 0 bps, 5 minutes 0 bps
    output average rate: 30 seconds 0 bps, 5 minutes 0 bps
  Time since last state change: 0 days 00:00:07
```


**Related
commands** [interface tunnel \(IPsec\)](#)

show ipsec counters

Overview Use this command to show IPsec counters.

Syntax show [crypto] ipsec counters

Parameter	Description
crypto	Security specific command.
ipsec	Internet Protocol Security defines the protection of IP packets using encryption and authentication.
counters	Show IPsec transformation statistic.

Mode Privileged Exec

Examples To show IPsec counters, enter the command below:

```
awplus# show ipsec counters
```

Output Figure 65-4: Example output from the **show ipsec counters** command

awplus#show ipsec counters	
Name	Value

InError	0
InBufferError	0
InHdrError	0
InNoStates	0
InStateProtoError	0
InStateModeError	0
InStateSeqError	0
InStateExpired	0
InStateMismatch	0
InStateInvalid	0
InTmplMismatch	0
InNoPols	0
InPolBlock	0
InPolError	0
OutError	0
OutBundleGenError	0
OutBundleCheckError	0
OutNoStates	0
OutStateProtoError	0
OutStateModeError	0
OutStateSeqError	0
OutStateExpired	0
OutPolBlock	0
OutPolDead	0
OutPolError	0
FwdHdrError	0

show ipsec peer

Overview Use this command to show IPsec information on a per peer basis.

Syntax show [crypto] ipsec peer [<hostname>|<ipv4-addr>|<ipv6-addr>]

Parameter	Description
crypto	Security specific command.
peer	Remote endpoint.
<hostname>	Destination hostname.
<ipv4-addr>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	Destination IPv6 address. The IPv6 address uses the format X:X::X:X.

Mode Privileged Exec

Examples To show IPsec information on a per peer basis, enter the command below:

```
awplus# show ipsec peer 172.16.0.1
```

Output Figure 65-5: Example output from the **show ipsec peer** command

```
awplus#show ipsec peer 172.16.0.1
172.16.0.2
IPsec
  Selectors (local:remote)
    Address: 0.0.0.0/0 : 0.0.0.0/0
    Protocol: any:any
    Port: any:any
    Mark: 1:1
  Profile: default
  SAs:
    SPI (In:Out): ca865389:c9c7e3d3
    Selectors: 192.168.1.0/24 : 192.168.2.0/24
    Proto: ESP
    Mode: tunnel
    Encryption: AES256
    Integrity: SHA256
    Expires: 28796s
ISAKMP
  LocalID: 172.16.0.1
  RemoteID: 172.16.0.2
  SAs:
    Cookies (Initiator:Responder) 03071749781e5992:93f8457816d3d40d
    Ver: 2 Lifetime: 84569s State: Established
    Authentication: PSK Group: 14
    Encryption: AES256 NATT: no
    Integrity: SHA256 DPD: yes
```

show ipsec policy

Overview Use this command to show IPsec policies.

Syntax `show [crypto] ipsec policy`

Parameter	Description
crypto	Security specific command.
ipsec	Internet Protocol Security defines the protection of IP packets using encryption and authentication.
policy	Policy.

Mode Privileged Exec

Examples To show IPsec policies, enter the command below:

```
awplus# show ipsec policy
```

Output Figure 65-6: Example output from the **show ipsec policy** command

```
awplus#show ipsec policy
Traffic Selector (addresses protocol ports interface)
  Profile      Peer
0.0.0.0/0 0.0.0.0/0  tunnel1
default      10.2.0.10
```

show ipsec profile

Overview Use this command to show IPsec default and custom profiles.

An IPsec profile consists of a set of parameters that are used by IPsec when establishing IPsec SAs with a remote peer. AlliedWare Plus provides default ISAKMP and IPsec profiles that contain a priority ordered set of transforms that are considered secure by the security community.

Syntax `show [crypto] ipsec profile [<profile_name>]`

Parameter	Description
crypto	Security specific.
ipsec	Internet Protocol Security defines the protection of IP packets using encryption and authentication.
profile	An IPsec profile consists of a set of parameters that are used by IPsec SAs with a remote peer.
<profile_name>	Custom profile name.

Mode Privileged Exec

Examples To show all IPsec profiles, including the default profile, use the following command:

```
awplus# show ipsec profile
```

Output Figure 65-7: Example output from the **show ipsec profile** command

```
awplus#show ipsec profile
IPsec Profile: default
  Replay-window: 32
  Rekey: Always
  Expiry: 8h
  PFS group: disabled
  Transforms:
  Protocol Integrity Encryption
    1 ESP SHA256 AES256
    2 ESP SHA1 AES256
    3 ESP SHA256 AES128
    4 ESP SHA1 AES128
    5 ESP SHA256 3DES
    6 ESP SHA1 3DES

IPsec Profile: my_profile
  Replay-window: 32
  Rekey: On Demand
  Expiry: 8h
  PFS group: disabled
  Transforms:
  Protocol Integrity Encryption
    2 ESP SHA1 3DES
```

Examples To show IPsec profile “my_profile”, use the command:

```
awplus# show ipsec profile my_profile
```

Output Figure 65-8: Example output from the **show ipsec profile** command

```
awplus#show ipsec profile my_profile
IPsec Profile: my_profile
  Replay-window: 32
  Rekey: On Demand
  Expiry: 8h
  PFS group: disabled
  Transforms:
  Protocol Integrity Encryption
    2 ESP SHA1 3DES
```

Related commands [crypto ipsec profile](#)

show ipsec sa

Overview Use this command to view the settings used by current security associations. SAs specify the Security Parameter Index (SPI), protocols, algorithms and keys for protecting a single flow of traffic between two IPsec peers. For more information about SA, see the [Internet Protocol Security \(IPSec\) Feature Overview and Configuration Guide](#).

Syntax show [crypto] ipsec sa

Parameter	Description
crypto	Security specific command.
ipsec	Internet Protocol Security defines the protection of IP packets using encryption and authentication.
sa	Security Association.

Mode Privileged Exec

Examples To view the settings used by current security associations, enter the command below:

```
awplus# show ipsec sa
```

Output Figure 65-9: Example output from the **show ipsec sa** command

awplus#show ipsec sa				
Peer	SPI (in:out) Encryption	Mode Integrity	Proto PFS	Expires
10.0.0.20	c2d8c150:7b24d3f5 AES256	tunnel SHA256	ESP -	28786s
10.0.0.22	c6c2ad0d:0d008e3d 3DES	tunnel SHA1	ESP -	3582s
10.0.0.25	cb36f9dd:cd87a834 AES128	tunnel SHA1	ESP 2	28778s

show isakmp counters

Overview Use this command to show ISAKMP counters.

Syntax show [crypto] isakmp counters

Parameter	Description
crypto	Security specific command.
isakmp	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
counters	Show ISAKMP counters.

Mode Privileged Exec

Examples To show ISAKMP counters, enter the command below:

```
awplus# show isakmp counters
```

Output Figure 65-10: Example output from the **show isakmp counters** command

awplus#show isakmp counters	
Name	Value
-----	-----
ikeInitRekey	0
ikeRspRekey	0
ikeChildSaRekey	0
ikeInInvalid	0
ikeInInvalidSpi	0
ikeInInitReq	0
ikeInInitRsp	0
ikeOutInitReq	0
ikeOutInitRsp	0
ikeInAuthReq	0
ikeInAuthRsp	0
ikeOutAuthReq	0
ikeOutAuthRsp	0
ikeInCrChildReq	0
ikeInCrChildRsp	0
ikeOutCrChildReq	0
ikeOutCrChildRsp	0
ikeInInfoReq	0
ikeInInfoRsp	0
ikeOutInfoReq	0
ikeOutInfoRsp	0

show isakmp key (IPsec)

Overview Use this command to show ISAKMP authentication keys. These keys can be of type Pre-shared Key (PSK) or Extensible Authentication Protocol (EAP). Keys are stored encrypted in the running-configuration.

Syntax `show [crypto] isakmp key`

Parameter	Description
crypto	Security specific command.
isakmp	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
key	Pre-shared key (PSK), or Extensible Authentication Protocol (EAP).

Mode Privileged Exec

Examples To show the ISAKMP keys, enter the command below:

```
awplus# show isakmp key
```

Output Figure 65-11: Example output from the **show isakmp key** command

awplus#show isakmp key		
Hostname/IP address	PSK	EAP

10.1.1.1	mykeyone	mykeytwo
10.1.5.1	mykeyfive	-
10.1.7.1	-	mykeyseven

Related commands [crypto isakmp key](#)

show isakmp peer

Overview Use this command to show ISAKMP profile and key status for ISAKMP peers.

Syntax `show isakmp peer [<hostname>|<ipv4-addr>|<ipv6-addr>]`

Parameter	Description
<hostname>	Destination hostname.
<ipv4-addr>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	Destination IPv6 address. The IPv6 address uses the format X:X::X:X.

Mode Privileged Exec

Examples To show ISAKMP profile and key status for ISAKMP peers, use the following command:

```
awplus# show isakmp peer
```

Output Figure 65-12: Example output from the **show isakmp peer** command

awplus#show isakmp peer		
Peer	Profile (* incomplete)	Key

10.1.1.1	default	PSK, EAP
10.1.5.1	SECURE	PSK
example.com	LEGACY	EAP

Related commands [crypto isakmp peer](#)

Command changes Version 5.4.7-0.1: Parameter **hostname** added for DDNS feature.

show isakmp profile

Overview Use this command to show ISAKMP default and custom profiles.

Syntax `show [crypto] isakmp profile [<profile_name>]`

Parameter	Description
<profile_name>	Custom profile name.

Mode Privileged Exec

Examples To show ISAKMP profiles, including the default profile, use the command:

```
awplus# show isakmp profile
```

Output Figure 65-13: Example output from the **show isakmp profile** command

```
awplus#show isakmp profile
ISAKMP Profile: default
  Version:      IKEv2
  Authentication: PSK
  Expiry:       24h
  DPD Interval: 30s
  Transforms:
    Integrity  Encryption  DH Group
    1  SHA256   AES256    14
    2  SHA256   AES256    16
    3  SHA1     AES256    14
    4  SHA1     AES256    16
    5  SHA256   AES128    14
    6  SHA256   AES128    16
    7  SHA1     AES128    14
    8  SHA1     AES128    16
    9  SHA256   3DES      14
   10  SHA256   3DES      16
   11  SHA1     3DES      14
   12  SHA1     3DES      16

ISAKMP Profile: my_profile
  Version:      IKEv2
  Authentication: PSK
  Expiry:       24h
  DPD Interval: 30s
  Transforms:
    Integrity  Encryption  DH Group
    2  SHA1     3DES      5
```

Examples To show ISAKMP profile “my_profile”, use the command:

```
awplus# show isakmp profile my_profile
```

Output Figure 65-14: Example output from the **show isakmp profile** command

```
awplus#show isakmp profile my_profile
ISAKMP Profile: my_profile
Version:          IKEv2
Authentication:   PSK
Expiry:           24h
DPD Interval:     30s
Transforms:
    Integrity      Encryption  DH Group
    2    SHA1       3DES         5
```

Related commands [crypto isakmp profile](#)

show isakmp sa

Overview Use this command to show current IKE security associations at a peer.

Syntax show [crypto] isakmp sa

Parameter	Description
crypto	Security specific command.
isakmp	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
sa	Security Association.

Mode Privileged Exec

Examples To show current IKE security associations at a peer, enter the command below:

```
awplus# show isakmp sa
```

Output Figure 65-15: Example output from the **show isakmp sa** command

awplus#show isakmp sa						
Peer	Cookies (initiator:responder)			Auth	Ver	Expires
	Encryption	Integrity	Group	DPD	NATT	State
10.0.0.20	f93c2717a1ece407:972bc0c77344d7a4			PSK	1	78340s
	AES256	SHA256	2	yes	no	Established
10.0.0.22	ccb7f90b54945375:2642525bd20f3428			PSK	1	3334s
	3DES	SHA1	2	yes	no	Established
10.0.0.25	bd0efef134c86656:d46d0b1b72b46444			PSK	1	819s
	AES128	SHA1	2	yes	no	Established

show tunnel inline-processing counters

Overview Use this command to show the tunnel inline-processing counters.

Syntax `show tunnel inline-processing counters`

Mode Privileged Exec

Usage notes Global counters show packet counts (esp, frames, nsh, oam), packet decisions (decrypts, drops), and IPsec SAs tracked by tunnel inline (msg_...,sa_added, sa_deleted).

Per worker counters show the packet counts and decisions made by each worker and activity counters (fetch, sleep, wakeup,...).

Example To display tunnel inline-processing counters, use the command:

```
awplus# show tunnel inline-processing counters
```

Output Figure 65-16: Example output from **show tunnel inline-processing counters**

```
show tunnel inline-processing counters
Global Counters:
      decrypts                4913089
      drop                    0
      err_not_esp              0
      err_trans_auth           0
      err_trans_crypto         0
      esp                     4913089
      esp_error_internal       0
      esp_error_invalid_hmac   0
      esp_error_malformed      0
      esp_error_replay_fail    0
      esp_no_sa                0
      espinudp                 0
      frames                   7518246
      ignore                   2605157
      msg_del_sa               0
      msg_expired_sa           0
      msg_flush_sa             0
      msg_new_sa               0
      msg_unknown              0
      msg_updated_sa           0
      nsh                      7518246
      oam                      0
      sa_added                 2
      sa_deleted               0...
```

worker0: sleeping	
decrypts	1386914
drop	0
esp	1386914
esp_error_internal	0
esp_error_invalid_hmac	0
esp_error_malformed	0
esp_error_replay_fail	0
esp_no_sa	0
espinudp	0
fetch00	617322
fetch01	407403
fetch02_03	155630
fetch04_07	36150
fetch08_15	11152
fetch16_31	2457
fetch32_63	2553
fetch64_	2787
frames	2669292
ignore	1282378
nsh	2669292
oam	0
return00	0
return01	407403
return02_03	155630
return04_07	36150
return08_15	11152
return16_31	2457
return32_63	2553
return64_	2787
sleep	617322
sleep_cmd	617322
sleep_user	0
sleep_work	617322
wakeup	617321
wakeup_cmd	0
wakeup_user	0
wakeup_work	617321

Related commands [tunnel inline-processing](#)

Command changes Version 5.5.2-1.1: command added

transform (IPsec Profile)

Overview Use this command to create an IPsec profile transform, which specifies the encryption and authentication algorithms used to protect data.

Use the **no** variant to delete a previously created transform.

Syntax

```
transform <1-255> protocol esp integrity {sha1|sha256|sha512}  
encryption {3des|aes128|aes192|aes256|null}  
  
transform <1-255> protocol esp integrity {gcm8|gcm12|gcm16}  
encryption {aes128|aes192|aes256}  
  
no transform <1-255>
```

Parameter	Description
<1-255>	Transform priority (1 is the highest).
sha1	Secure Hash Standard with 160-bit digest size.
sha256	Secure Hash Standard with 256-bit digest size.
sha512	Secure Hash Standard with 512 bit digest size.
3des	Triple DES symmetric key block cipher with a 168-bit key.
aes128	Advanced Encryption Standard symmetric key block cipher with a 128-bit key.
aes192	Advanced Encryption Standard symmetric key block cipher with a 192-bit key.
aes256	Advanced Encryption Standard symmetric key block cipher with a 256-bit key.
gcm8	Galois/Counter Mode that uses an 8-byte authentication tag.
gcm12	Galois/Counter Mode that uses a 12 byte authentication tag.
gcm16	Galois/Counter Mode that uses a 16 byte authentication tag.
null	No encryption. This option is not intended for use in a live network. It should only be used for testing purposes.

Default By default, an IPsec profile has no transforms and so will not be active.

Mode IPsec Profile Configuration

Examples To configure an IPsec profile transform, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile  
awplus(config-ipsec-profile)# transform 2 protocol esp  
integrity sha1 encryption 3des
```

To delete a created transform, use the following command:

```
awplus(config-ipsec-profile)# no transform 2
```


Related commands [crypto ipsec profile](#)

Validation Commands [show ipsec profile](#)

Command changes Version 5.5.3-2.1: **gcm** parameters added

transform (ISAKMP Profile)

Overview Use this command to create an ISAKMP profile transform which specifies the encryption and authentication algorithms used to protect data in the tunnel.

Use the **no** variant to delete a previously created transform.

Syntax `transform <1-255> integrity {sha1|sha256|sha512} encryption {3des|aes128|aes192|aes256} group {2|5|14|15|16|18}`
`no transform <1-255>`

Parameter	Description
<1-255>	Transform priority (1 is the highest)
sha1	Secure Hash Standard with 160-bit digest size
sha256	Secure Hash Standard with 256-bit digest size
sha512	Secure Hash Standard with 512 bit digest size
3des	Triple DES symmetric key block cipher with a 168-bit key
aes128	Advanced Encryption Standard symmetric key block cipher with a 128-bit key
aes192	Advanced Encryption Standard symmetric key block cipher with a 192-bit key
aes256	Advanced Encryption Standard symmetric key block cipher with a 256-bit key
group	Diffie-Hellman group
2	1024-bit MODP Group
5	1536-bit MODP Group
14	2048-bit MODP Group
15	3072-bit MODP Group
16	4096-bit MODP Group
18	8192-bit MODP Group

Default By default, an ISASMP profile has no transforms and so will not be active.

Mode ISAKMP Profile Configuration

Examples To create an ISAKMP profile transform, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# transform 2 integrity sha1
encryption 3des group 5
```

To delete a created transform, use the following command:

```
awplus(config-isakmp-profile)# no transform 2
```

**Related
commands** [crypto isakmp profile](#)

tunnel destination (IPsec)

Overview Use this command to specify a destination IPv4 or IPv6 address or destination network name for the remote end of the tunnel.

Use the **no** variant of this command to remove a configured tunnel destination address.

Syntax tunnel destination {<WORD>|<ipv4-address>|<ipv6-address>}
no tunnel destination {<WORD>|<ipv4-address>|<ipv6-address>}

Parameter	Description
<WORD>	Destination network name or “dynamic”. The “dynamic” parameter allows you to specify a dynamic IP address for the remote endpoint. The dynamic IP address can be obtained, for example, via DHCP.
<ipv4-address>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-address>	Destination IPv6 address. The IPv6 address uses the format X:X::X:X.

Mode Interface Configuration

Examples To configure a destination IPv4 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination 192.0.3.1
```

To configure a destination IPv6 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel destination 2001:0db8::
```

To configure a destination network name for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination www.example.com
```

To configure a dynamic IP address for the tunnel destination, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination dynamic
```

To remove the destination address of IPSec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# no tunnel destination 192.0.3.1
```

Related [tunnel source \(IPsec\)](#)
commands

tunnel inline-processing

Overview Use this command to configure tunnel inline-processing for an IPsec encrypted tunnel.

Tunnel inline-processing is a faster alternative to tunnel security-reprocessing which is the alternative, less efficient option. With tunnel security-reprocessing configured, the DPI engine processes incoming VPN traffic twice (before and after decryption), in order to identify incoming application traffic transported via an encrypted VPN.

Tunnel inline-processing is useful because it means packets are decrypted before being analysed and processed via the DPI engine. This is especially important for VPN traffic, where you actually want to identify application traffic transported within the IPsec VPN, rather than the outer encrypted IPsec VPN headers.

Use the **no** variant of this command to disable tunnel inline-processing for an IPsec encrypted tunnel.

Syntax `tunnel inline-processing`
`no tunnel inline-processing`

Default Disabled

Mode Interface Configuration

Example To enable tunnel inline-processing, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel inline-processing
```

To disable tunnel inline-processing, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# no tunnel inline-processing
```

Related commands [show tunnel inline-processing counters](#)

Command changes Version 5.5.2-1.1: command added

tunnel local name (IPsec)

Overview Use this command to specify an IPsec tunnel hostname to send to the peer for authentication when you apply [tunnel protection ipsec \(IPsec\)](#) to encrypt the packets and configure an ISAKMP key.

Use the **no** variant of this command to remove a previously configured IPsec tunnel hostname.

Syntax tunnel local name *<local-name>*
no tunnel local name

Parameter	Description
<i><local-name></i>	Source tunnel hostname.

Default The default tunnel local name is the IP address of tunnel source.

Mode Interface Configuration

Examples To configure the tunnel local name office1 for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel local name office1
```

To remove a configured tunnel local name for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel local name
```

Related commands [tunnel remote name \(IPsec\)](#)

tunnel local selector

Overview Use this command to specify a local subnet for a traffic selector pair.

Use the **no** variant of this command to unset the local subnet for the traffic selector pair so that it matches all sources, i.e. 0.0.0.0/0 or ::/0 for IPv4 and IPv6, respectively. When local and remote subnets for a traffic selector pair are both unset, the traffic selector pair is removed.

Syntax tunnel local selector [<traffic-selector-ID>]
{<ipv4-subnet>|<ipv6-subnet>}
no tunnel local selector [<traffic-selector-ID>]

Parameter	Description
<traffic-selector-ID>	Optional traffic selector ID from 1 through 65535. The default is 1.
<ipv4-subnet>	IPv4 subnet in the format A.B.C.D/M.
<ipv6-subnet>	IPv6 subnet in the format of X:X::X:X/M

Default When no traffic selector pairs are configured there is an implicit traffic selector pair, where the local and remote subnets are 0.0.0.0/0 or ::/0 depending on the tunnel IPsec mode.

Mode Interface configuration

Usage notes A traffic selector pair is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote subnets. When the local selector is specified but the remote selector is not, the selector pair implicitly matches all destinations.

Examples To specify an IPv4 destination address as the traffic selector for the traffic to match for tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth0
awplus(config-if)# tunnel destination 10.0.0.2
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel local selector 192.168.1.0/24
awplus(config-if)# tunnel remote selector 192.168.2.0/24
```


To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 192.168.1.0/24
awplus(config-if)# tunnel remote selector 5 192.168.2.0/24
```

To specify an IPv6 source address as the traffic selector for the traffic to match for tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth0
awplus(config-if)# tunnel destination 2001:db8:10::1
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel local selector 2001:db8:1::/64
awplus(config-if)# tunnel remote selector 2001:db8:2::/64
```

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 2001:db8:1::/64
awplus(config-if)# tunnel remote selector 5 2001:db8:2::/64
```

To unset the destination traffic selector for the traffic selector pair with ID 1, for tunnel 6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel remote selector

or

awplus(config-if)# no tunnel remote selector 1
```

**Related
commands**

[tunnel remote selector](#)

[tunnel selector paired](#)

[show interface tunnel \(IPsec\)](#)

tunnel mode ipsec

Overview Use this command to configure the encapsulation tunneling mode to use.
Use the **no** variant of this command to remove an established tunnel.

Syntax tunnel mode ipsec {ipv4|ipv6}
no tunnel mode

Parameter	Description
ipsec ipv4	IPv4 IPsec tunnel
ipsec ipv6	IPv6 IPsec tunnel

Default Virtual tunnel interfaces have no mode set.

Mode Interface Configuration

Usage notes A tunnel will not become operational until it is configured with this command.

Examples To configure IPsec in IPv4 tunnel mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel mode ipsec ipv4
```

To remove the configured IPsec tunnel mode for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel mode
```

tunnel oper-status-control

Overview Use this command to configure the control of operation status for point-to-point IPsec protected tunnels. This type of tunnel can be configured to use the presence or absence of an IPsec SA to determine if the interface should be considered 'UP' or 'DOWN'.

Use the **no** variant of this command to return a tunnel to the default configuration of not using the existence of an IPsec SA to set the oper-status of the tunnel.

Syntax tunnel oper-status-control {ipsec|none}
no tunnel oper-status-control

Parameter	Description
ipsec	Use the presence or absence of an IPsec SA, associated with an IPsec-protected tunnel to control the oper-status of the tunnel interface.
none	Always show the oper-status of the tunnel as 'Link is UP' and 'RUNNING'.

Default None.

Mode Interface Configuration

Usage notes By default, when a tunnel is fully configured and is administratively enabled, the tunnel always shows 'Link is UP' and the RUNNING flag is always set in the output of the **show interface** command. This is because tunnels are virtual interfaces that have no electrical state associated with them. However, this does not mean that the tunnel is capable of passing traffic.

In order to provide a kind of oper-status for point-to-point IPsec protected tunnels, the tunnel can be configured to use the presence or absence of an IPsec SA to determine if the interface should be considered 'UP' or 'DOWN', respectively. When configured in this way the device will always attempt to maintain an IPsec SA with the remote device, whereas normally one would only be established if there is traffic that needs to be passed. This is necessary, otherwise routes over the tunnel would not be considered active.

Example To use the presence of IPsec SA's to control the oper-status of interface 'tunnel1', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# tunnel oper-status-control ipsec
```

Output 1 Figure 65-17: Example output from **show interface tunnel1**

In this first example, there is an IPsec SA (i.e. IPsec has negotiated and is ready to send data) and so the link shows as 'UP'.

```
awplus#show interface tunnel1
Interface tunnel1
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 10.1.1.1/24 point-to-point 10.1.1.255
  index 17 metric 1 mtu 1438
UP, POINT-TO-POINT, RUNNING, MULTICAST
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Tunnel source eth1 (172.16.1.1), destination 172.16.1.2
  Tunnel name local 172.16.1.1, remote 172.16.1.2
  Tunnel traffic selectors (ID, local, remote)
    1    0.0.0.0/0                0.0.0.0/0
  Tunnel protocol/transport ipsec ipv4, key disabled, sequencing disabled
  Checksumming of packets disabled, DF bit set, path MTU discovery disabled
  Tunnel protection via IPsec (profile "default")
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 0, bytes 0, dropped 0, multicast packets
    output packets 0, bytes 0, multicast packets 0, broadcast packets 0
    input average rate : 30 seconds 0 bps, 5 minutes 0 bps
    output average rate: 30 seconds 0 bps, 5 minutes 0 bps
  Time since last state change: 0 days 00:00:49
...
```

Output 2 Figure 65-18: Example output from **show interface tunnel1**

In the second example there is no IPsec SA and so the link is 'DOWN'.

```
awplus#show interface tunnel1
Interface tunnel1
  Link is DOWN, administrative state is UP
  Hardware is Tunnel
  IPv4 address 10.1.1.1/24 point-to-point 10.1.1.255
  index 17 metric 1 mtu 1438
UP, POINT-TO-POINT, MULTICAST
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Tunnel source eth1 (172.16.1.1), destination 172.16.1.2
  Tunnel name local 172.16.1.1, remote 172.16.1.2
  Tunnel traffic selectors (ID, local, remote)
    1    0.0.0.0/0                0.0.0.0/0
  Tunnel protocol/transport ipsec ipv4, key disabled, sequencing disabled
  Checksumming of packets disabled, DF bit set, path MTU discovery disabled
  Tunnel protection via IPsec (profile "default")
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 0, bytes 0, dropped 0, multicast packets
    output packets 0, bytes 0, multicast packets 0, broadcast packets 0
    input average rate : 30 seconds 0 bps, 5 minutes 0 bps
    output average rate: 30 seconds 0 bps, 5 minutes 0 bps
  Time since last state change: 0 days 00:00:49
...
```

**Related
commands** [show interface](#)

**Command
changes** Version 5.5.1-2.1: command added

tunnel protection ipsec (IPsec)

Overview Use this command to enable IPsec protection for packets encapsulated by this tunnel.

Use the **no** variant to disable IPsec protection.

Syntax `tunnel protection ipsec [profile <profile_name>]`
`no tunnel protection ipsec`

Default IPsec protection for packets encapsulated by tunnel is disabled. If no custom profile is specified, the default profile is used.

Parameter	Description
<profile_name>	Custom profile name. You can use the crypto ipsec profile command to create custom profiles.

Mode Interface Configuration

Usage notes IPsec mode tunnels (IPv4 and IPv6) require this command for them to work. GRE IPv6 and L2TPv3 IPv6 tunnel have IPsec protection as an option.

Examples To enable IPsec protection by using default profile, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# tunnel protection ipsec
```

To enable IPsec protection by using a custom profile, use the following commands:

```
awplus(config)# interface tunnel14
awplus(config-if)# tunnel protection ipsec profile
my_profile
```

To disable IPsec protection for packets encapsulated by tunnel14, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# no tunnel protection ipsec
```

Related commands [crypto ipsec profile](#)

tunnel remote name (IPsec)

Overview Use this command to specify a tunnel remote name to authenticate the tunnel's remote peer device when you apply [tunnel protection ipsec \(IPsec\)](#) to encrypt the packets and configure an ISAKMP key.

Use the **no** variant of this command to remove a previously configured tunnel remote name.

Syntax `tunnel remote name <remote-name>`
`no tunnel local name`

Parameter	Description
<code><remote-name></code>	Destination tunnel hostname

Default The default tunnel remote name is the IP address of tunnel destination.

Mode Interface Configuration

Examples To configure tunnel remote name office2 for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel remote name office2
```

To remove a configured tunnel local name for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel remote name
```

Related commands [tunnel local name \(IPsec\)](#)

tunnel remote selector

Overview Use this command to specify a destination subnet for a traffic selector pair.

Use the **no** variant of this command to unset the remote subnet for a traffic selector pair so that it matches all destinations, i.e. 0.0.0.0/0 or ::/0 for IPv4 and IPv6, respectively. When local and remote subnets for a traffic selector pair are both unset, the traffic selector pair is removed.

Syntax `tunnel remote selector [<traffic-selector-ID>]
{<IPv4-subnet>|<IPv6-subnet>}`

`no tunnel remote selector [<traffic-selector-ID>]`

Parameter	Description
<traffic-selector-ID>	Traffic selector ID from 1 through 65535. If not specified the default value 1 is used.
<ipv4-subnet>	IPv4 subnet in the format A.B.C.D/M.
<ipv6-subnet>	IPv6 subnet in the format of X:X::X/M

Default When no traffic selector pairs are configured there is an implicit traffic selector pair, where the local and remote subnets are 0.0.0.0/0 or ::/0 depending on the tunnel IPsec mode.

Mode Interface configuration

Usage notes A traffic selector pair is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote subnets. When the remote selector is specified but the local selector is not, the selector pair implicitly matches all sources.

Examples To specify an IPv4 destination address as the traffic selector for the traffic to match for tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth0
awplus(config-if)# tunnel destination 10.0.0.2
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel local selector 192.168.1.0/24
awplus(config-if)# tunnel remote selector 192.168.2.0/24
```

When no traffic selector ID is specified the default ID value is used. By specifying a traffic selector ID, additional selector pairs can be configured.

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 192.168.1.0/24
awplus(config-if)# tunnel remote selector 5 192.168.2.0/24
```

To specify an IPv6 source address as the traffic selector for the traffic to match for tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth0
awplus(config-if)# tunnel destination 2001:db8:10::1
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel local selector 2001:db8:1::/64
awplus(config-if)# tunnel remote selector 2001:db8:2::/64
```

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 2001:db8:1::/64
awplus(config-if)# tunnel remote selector 5 2001:db8:2::/64
```

To unset the destination traffic selector for the traffic selector pair with ID 1, for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel remote selector
```

or

```
awplus(config-if)# no tunnel remote selector 5
```

**Related
commands**

[tunnel local selector](#)

[tunnel selector paired](#)

[show interface tunnel \(IPsec\)](#)

tunnel security-reprocessing

Overview Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

Syntax `tunnel security-reprocessing`
`no tunnel security-reprocessing`

Default Security reprocessing is disabled by default.

Mode Global Configuration

Usage notes Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#).

Example To enable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# no tunnel security-reprocessing
```

Related commands [show interface tunnel \(GRE\)](#)
[show interface tunnel \(IPsec\)](#)
[show interface tunnel \(L2TPv3\)](#)
[show interface tunnel \(OpenVPN\)](#)

Command changes Version 5.4.8-0.2: command added

tunnel selector paired

Overview Use this command when multiple selector pairs are configured. This command forces ISAKMP to use strict pairing and therefore create separate Phase 2 IPsec SAs between pairs of source and destination selectors, based on selector ID.

Use the **no** variant of this command to stop forcing strict selector ID pairing.

Syntax `tunnel selector paired`

Default Disabled

Mode Interface mode for a tunnel

Usage notes When this command is disabled, if you specify address selectors, the tunnel can permit any combination of matching sources and/or destinations. While this conforms to the RFC, it may not be the expected behavior and may cause the IPsec SA to either fail negotiation or fail to pass traffic correctly.

This command forces ISAKMP to create individual IPsec SAs for each pair of source and destination selectors that have the same selector ID. Only traffic that matches a selector pair is permitted to flow via the associated SA.

Example To create a tunnel between 172.16.1.0/24 and 172.16.2.0/24, and also between 172.16.1.0/24 and any other destination, use the following tunnel selector commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel local selector 2 172.16.1.0/24
awplus(config-if)# tunnel remote selector 2 172.16.2.0/24
awplus(config-if)# tunnel local selector 3 172.16.1.0/24
awplus(config-if)# tunnel remote selector 3 0.0.0.0/0
awplus(config-if)# tunnel selector paired
```

Related commands [tunnel local selector](#)
[tunnel remote selector](#)
[show interface tunnel \(IPsec\)](#)

Command changes Version 5.4.8-1.1: command added

tunnel source (IPsec)

Overview Use this command to specify an IPv4 or IPv6 source address or interface name for packets being encapsulated in the IPsec tunnel. The source address should be an existing IPv4 address or IPv6 address or interface name configured for an interface.

Note that if the tunnel source interface has multiple IP addresses, for example, one primary and one or more secondary IP addresses, the lowest IP address on the interface is used for transporting the tunnel encapsulated traffic.

Use the **no** variant of this command to remove a tunnel source address for a tunnel interface.

Syntax `tunnel source {<interface-name>|<ipv4-address>|<ipv6-address>}`
`no tunnel source`
`{<interface-name>|<ipv4-address>|<ipv6-address>}`

Parameter	Description
<interface-name>	Interface name.
<ipv4-address>	The IPv4 address uses the format A.B.C.D.
<ipv6-address>	The IPv6 address uses the format X:X::X:X.

Mode Interface Configuration

Examples To configure a source IPv4 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel source 192.168.1.1
```

To configure a source IPv6 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel source 2001:db8::
```

To configure a source interface for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel source eth0
```

To remove the source address of IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# no tunnel source 192.168.1.1
```

Related commands [tunnel destination \(IPsec\)](#)

undebg isakmp

Overview Use this command to disable debugging ISAKMP.

To enable debugging ISAKMP, see [debug isakmp](#).

Syntax undebg [crypto] isakmp [info|trace|all]

Parameter	Description
undebg	Disable debugging function.
crypto	Security specific command.
isakmp	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
info	Informational debug messages such as protocol events.
trace	Verbose debug messages including protocol events and message traces.
all	All debug enabled.

Mode Privileged Exec

Related commands [debug isakmp](#)
[no debug isakmp](#)

version (ISAKMP)

Overview Use this command to set the ISAKMP protocol version.
Use the **no** variant to set the protocol version to default (IKEv2).

Syntax `version {1 mode {aggressive|main}|2}`
`no version`

Parameter	Description
1	IKEv1
main	IKEv1 Main mode. An IKE session begins with the initiator and recipient sending three two-way exchanges to define what encryption and authentication protocols are acceptable, how long keys should remain active, and whether perfect forward secrecy should be enforced. Main mode uses more packets for the process than Aggressive mode, but Main mode is considered more secure.
aggressive	IKEv1 Aggressive mode. The initiator and recipient accomplish the same objectives, but in only two exchanges.
2	IKEv2

Default If you do not specify the version, the default version is IKEv2

Mode IPsec ISAKMP Configuration

Examples To set the ISAKMP protocol version of profile "my_profile" to IKEv1 main mode, use the following commands:

```
awplus(config)# configure isakmp profile my_profile
awplus(config-isakmp-profile)# version 1 mode main
```

To set the version to its default, use the following command:

```
awplus# no version
```

Related commands [crypto isakmp profile](#)

Validation Commands [show isakmp profile](#)

66

GRE Tunneling Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure IPv6 tunnels. For more information about IPv6 tunnels, see the [Generic Routing Encapsulation \(GRE\) Feature Overview and Configuration Guide](#).

- Command List**
- “[interface tunnel \(GRE\)](#)” on page 2781
 - “[local authentication](#)” on page 2782
 - “[remote authentication](#)” on page 2784
 - “[show interface tunnel \(GRE\)](#)” on page 2786
 - “[tunnel checksum](#)” on page 2787
 - “[tunnel dscp](#)” on page 2788
 - “[tunnel destination \(GRE\)](#)” on page 2789
 - “[tunnel endpoint](#)” on page 2791
 - “[tunnel local name \(GRE\)](#)” on page 2793
 - “[tunnel mode gre](#)” on page 2794
 - “[tunnel mode gre multipoint](#)” on page 2795
 - “[tunnel protection ipsec \(GRE\)](#)” on page 2796
 - “[tunnel remote name \(GRE\)](#)” on page 2797
 - “[tunnel security-reprocessing](#)” on page 2798
 - “[tunnel source \(GRE\)](#)” on page 2799
 - “[tunnel ttl](#)” on page 2801

interface tunnel (GRE)

Overview Use this command to create a tunnel interface or to enter Interface mode to configure an existing tunnel. Tunnel interfaces are identified by an index identifier that is an integer in the range from 0 through 65535.

Use the **no** variant of this command to remove a previously created tunnel interface.

Syntax `interface tunnel<0-65535>`
`no interface tunnel<tunnel-index>`

Parameter	Description
<code><0-65535></code>	Specify a tunnel interface index identifier in the range from 0 through 65535.

Default Tunnel interfaces do not exist.

Mode Global Configuration

Usage notes After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

Examples To configure a tunnel interface with index 30 and enable GRE, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel30
awplus(config-if)# tunnel mode gre
```

To remove the GRE tunnel interface tunnel30, use the commands:

```
awplus# configure terminal
awplus(config)# no interface tunnel30
```

Command changes Version 5.4.7-2.1: increased range for **tunnel** index identifiers.

local authentication

Overview Use this command to specify the authentication method for the local device for a GRE Multipoint tunnel.

Use the **no** variant of this command to set the local authentication for an ISAKMP profile back to the default pre-shared.

Syntax `local authentication [pre-shared|eap-radius]`
`no local authentication`

Parameter	Description
pre-shared	Authenticate using pre-shared keys (default)
eap-radius	Authenticate using a radius server

Default Pre-shared

Mode ISAKMP Profile configuration

Usage notes This command allows you to choose between pre-shared, where a fixed key is known by both ends and eap-radius, where a key is stored on a radius server.

- Local authentication can be reset back to pre-shared (the default) for the device to authenticate using pre-shared keys.
- Local authentication can be set to eap-radius for the device to authenticate using a radius server.

Examples To configure local authentication for an ISAKMP profile, use the commands:

```
awplus# configure terminal
awplus(config)# configure isakmp profile my_profile
awplus(config-isakmp-profile)# local authentication eap-radius
```

To set the local authentication for an ISAKMP profile back to the default (pre-shared), use the commands:

```
awplus# configure terminal
awplus(config)# configure isakmp profile my_profile
awplus(config-isakmp-profile)# no local authentication
```

Related commands [remote authentication](#)
[show interface tunnel \(GRE\)](#)
[show isakmp profile](#)
[tunnel endpoint](#)
[tunnel mode gre multipoint](#)

Command changes Version 5.4.9-0.1: command added

remote authentication

Overview Use this command to specify the authentication method for the remote device for a GRE Multipoint tunnel.

Use the **no** variant of this command to set the remote authentication back to the default (pre-shared).

Syntax `remote authentication [pre-shared|eap-radius]`
`no remote authentication`

Parameter	Description
pre-shared	Authenticate using pre-shared keys (default)
eap-radius	Authenticate using a radius server

Default Pre-shared

Mode ISAKMP profile configuration

Usage notes This command allows you to choose between pre-shared, where a fixed key is known by both ends and eap-radius, where a key is stored on a radius server.

- Remote authentication can be reset back to pre-shared (the default) for the device to authenticate using pre-shared keys.
- Remote authentication can be set to eap-radius for the device to authenticate using a radius server.

Examples To configure remote authentication for an ISAKMP profile, use the following commands:

```
awplus# configure terminal
awplus(config)# configure isakmp profile my_profile
awplus(config-isakmp-profile)# remote authentication
eap-radius
```

To configure remote authentication for an ISAKMP profile back to the default (pre-shared), use the following commands:

```
awplus# configure terminal
awplus(config)# configure isakmp profile my_profile
awplus(config-isakmp-profile)# no remote authentication
```

Related commands [local authentication](#)
[show interface tunnel \(GRE\)](#)
[show isakmp profile](#)
[tunnel endpoint](#)

tunnel mode gre multipoint

Command changes Version 5.4.9-0.1: command added

show interface tunnel (GRE)

Overview Use this command to display status information of tunnels.

The tunnel remains inactive if no valid tunnel source or tunnel destination is configured.

Syntax `show interface tunnel< tunnel-index>`

Parameter	Description
tunnel	Specify this parameter to display tunnel status information of a given tunnel identified by the <0-65535> parameter.
<0-65535>	Specify a tunnel index in the range from 0 through 65535.

Mode Privileged Exec

Example To display status information for GRE tunnel tunnel20, use the command:

```
awplus# show interface tunnel20
```

Figure 66-1: Example output from the **show interface tunnel** command

```
awplus#show interface tunnel20
Interface tunnel20
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 172.16.1.1/24 pointopoint 172.16.1.255
  index 4750 metric 1 mtu 1480
  arp ageing timeout 300
  <UP,POINTOPOINT,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Tunnel source 192.168.1.1, destination 192.168.2.1
  Tunnel local 192.168.1.1, remote 192.168.2.1
  Tunnel protocol/transport gre, key disabled, sequencing disabled
  Tunnel TTL inherit
  Checksumming of packets disabled, path MTU discovery disabled
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast
  packets 0
  Time since last state change: 0 days 00:05:25
```

tunnel checksum

Overview Use this command to enable GRE tunnel checksum insertion and checking. This results in the first two bytes after the protocol field in the IPv4 header containing the checksum. The tunnel checksum is used to detect packet corruption.

Use the **no** variant of this command to disable checksum insertion and checking.

Syntax tunnel checksum
no tunnel checksum

Default Checksum insertion and checking is disabled.

Mode Interface Configuration

Examples To enable checksum insertion and checking, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode gre
awplus(config-if)# tunnel checksum
```

To disable checksum insertion and checking, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel checksum
```

tunnel dscp

Overview Use this command to configure the Differentiated Services Code Point (DSCP) value for the DSCP field in the packet header that encapsulates the tunneled packets.

Use the **no** variant of this command to reset the DSCP field to its default value.

Syntax `tunnel dscp <0-63>`
`no tunnel dscp`

Parameter	Description
<0-63>	Specify the DSCP value in the range from 0 through 63 for the DSCP field in the packet header that encapsulates the tunneled packets.

Default The IPv4 DSCP field value is inherited from the inner header to the outer header.

Mode Interface Configuration

Examples To configure the DSCP value to 10 for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel dscp 10
```

To remove a configured DSCP value for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel dscp
```

Related commands [interface tunnel \(IPv6\)](#)
[interface tunnel \(GRE\)](#)

tunnel destination (GRE)

Overview Use this command to specify a tunnel destination for the remote end of the tunnel. Tunnel destination can be specified by using a destination network name or an IPv4 address.

Use the **no** variant of this command to remove a configured tunnel destination.

Syntax `tunnel destination {<ipv4-addr>|<destination-network-name>}`
`no tunnel destination`

Parameter	Description
<code><ipv4-addr></code>	Specify the tunnel destination IPv4 address in the dotted decimal format A.B.C.D. The endpoints of the tunnel must be configured by mirroring IP addresses, that is, the tunnel source on one endpoint must be specified as the tunnel destination on the other endpoint.
<code><destination-network-name></code>	Destination network name. If the destination network name cannot be resolved, then the GRE tunnel remains inactive.

Mode Interface Configuration

Examples To configure an IPv4 tunnel destination by using an IPv4 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode gre
awplus(config-if)# tunnel destination 2.2.2.2
```

To configure a GRE tunnel destination by using a destination network name, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode gre
awplus(config-if)# tunnel destination
corporate_lan.example.com
```

To remove a GRE tunnel destination, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# no tunnel destination
```

**Related
commands** interface tunnel (GRE)
 tunnel mode gre
 tunnel source (GRE)

tunnel endpoint

Overview Use this command to set an endpoint to a GRE Multipoint tunnel interface.
Use the **no** variant of this command to remove an existing configured endpoint.

Syntax `tunnel endpoint {<ipv4-addr>|<network-name>|dynamic}`
`no tunnel endpoint {<ipv4-addr>|<network-name>|dynamic}`

Parameter	Description
<ipv4-address>	Specify the tunnel endpoint IPv4 address in the dotted decimal format A.B.C.D.
<network-name>	Specify the endpoint network name.
dynamic	Dynamically learn tunnel endpoints.

Default Virtual tunnel interfaces have no endpoints set.

Mode Interface Configuration

Examples To configure an IPv4 tunnel endpoint for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel endpoint 192.168.100.1
```

To remove the IPv4 tunnel endpoint for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel endpoint 192.168.100.1
```

To configure a tunnel endpoint network name "example_lan.com" for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel endpoint example_lan.com
```

To remove the tunnel endpoint network name "example_lan.com" for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel endpoint example_lan.com
```

To configure a dynamic tunnel endpoint for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel endpoint dynamic
```

To remove the dynamic tunnel endpoint for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel endpoint dynamic
```

**Related
commands**

[local authentication](#)
[remote authentication](#)
[show interface tunnel \(GRE\)](#)
[tunnel mode gre multipoint](#)

**Command
changes**

Version 5.4.9-0.1: command added

tunnel local name (GRE)

Overview Use this command to specify an IPsec tunnel hostname to send to the peer for authentication when you apply [tunnel protection ipsec \(GRE\)](#) to encrypt the packets and configure an ISAKMP key.

Use the **no** variant of this command to remove a previously configured IPsec tunnel hostname.

Syntax tunnel local name *<local-name>*
no tunnel local name

Parameter	Description
<i><local-name></i>	Source tunnel hostname.

Default The default tunnel local name is the IP address of tunnel source.

Mode Interface Configuration

Examples To configure the tunnel local name office1 for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel local name office1
```

To remove a configured tunnel local name for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel local name
```

Related commands [tunnel remote name \(GRE\)](#)

tunnel mode gre

Overview Use this command to configure the encapsulation tunneling mode to use. This command sets GRE IPv4 or IPv6 as the payload over IPv4 or IPv6 tunneling.

Use the **no** variant of this command to remove an established tunnel.

Syntax `tunnel mode gre [ipv6]`
`no tunnel mode`

Parameter	Description
<code>gre ipv6</code>	Specify GRE IPv4 or IPv6 as the payload over IPv6 tunneling. IPv6 is the delivery protocol.

Default Virtual tunnel interfaces have no mode set by default. If you specify a mode of **gre**, the delivery protocol is IPv4 unless you specify IPv6.

Mode Interface Configuration

Usage notes A tunnel will not become operational until it is configured with this command.

Examples To configure GRE as the encapsulation mode for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode gre
```

To remove a configured GRE tunnel mode for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel mode
```

Related commands [interface tunnel \(GRE\)](#)

tunnel mode gre multipoint

- Overview** Use this command to set the tunnel mode to GRE Multipoint.
Use the **no** variant of this command to unconfigure this tunnel mode.
- Syntax** `tunnel mode gre multipoint`
`no tunnel mode`
- Default** Virtual tunnel interfaces have no mode set.
- Mode** Interface Configuration
- Examples** To configure gre multipoint tunnel mode for tunnel6, use the commands:
- ```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel mode gre multipoint
```
- To remove the configured gre multipoint tunnel mode for tunnel6, use the commands:
- ```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel mode
```
- Related commands** [aaa authentication isakmp](#)
[crypto isakmp key](#)
[local authentication](#)
[remote authentication](#)
[show interface tunnel \(GRE\)](#)
[tunnel endpoint](#)
- Command changes** Version 5.4.9-0.1: command added

tunnel protection ipsec (GRE)

Overview Use this command to optionally enable IPsec protection for packets encapsulated by this tunnel.

Use the **no** variant to disable IPsec protection.

Syntax `tunnel protection ipsec [profile <ipsec-profile>]`
`no tunnel protection ipsec`

Parameter	Description
<ipsec-profile>	The name of an optional custom IPsec profile (crypto ipsec profile command) to use to protect this tunnel.

Default IPsec protection for packets encapsulated by tunnel is disabled.

Mode Interface Configuration

Usage notes You also need to configure a pre-shared key in conjunction with this command. See the [crypto isakmp key](#) command for more information about configuring the pre-shared key.

Examples To enable IPsec protection for packets encapsulated by `tunnel14`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# tunnel protection ipsec
```

To disable IPsec protection for packets encapsulated by `tunnel14`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# no tunnel protection ipsec
```

Related commands [crypto ipsec profile](#)
[crypto isakmp key](#)
[show isakmp key \(IPsec\)](#)

tunnel remote name (GRE)

Overview Use this command to specify a tunnel remote name to authenticate the tunnel's remote peer device when you apply [tunnel protection ipsec \(GRE\)](#) to encrypt the packets and configure an ISAKMP key.

Use the **no** variant of this command to remove a previously configured tunnel remote name.

Syntax `tunnel remote name <remote-name>`
`no tunnel local name`

Parameter	Description
<code><remote-name></code>	Destination tunnel hostname

Default The default tunnel remote name is the IP address of tunnel destination.

Mode Interface Configuration

Examples To configure tunnel remote name `office2` for `tunnel6`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel remote name office2
```

To remove a configured tunnel local name for `tunnel6`, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel remote name
```

Related commands [tunnel local name \(GRE\)](#)

tunnel security-reprocessing

Overview Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

Syntax `tunnel security-reprocessing`
`no tunnel security-reprocessing`

Default Security reprocessing is disabled by default.

Mode Global Configuration

Usage notes Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#).

Example To enable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# no tunnel security-reprocessing
```

Related commands [show interface tunnel \(GRE\)](#)
[show interface tunnel \(IPsec\)](#)
[show interface tunnel \(L2TPv3\)](#)
[show interface tunnel \(OpenVPN\)](#)

Command changes Version 5.4.8-0.2: command added

tunnel source (GRE)

Overview Use this command to specify a tunnel source for the tunnel interface. Tunnel source can be specified by using an interface name or an IPv4 address. The source address must be an existing IPv4 address configured for an interface.

Use the **no** variant of this command to remove a tunnel source for a tunnel interface.

Syntax tunnel source {<ipv4-addr>|<interface-name>}
no tunnel source

Parameter	Description
<ipv4-addr>	Specify the tunnel source IPv4 address for the GRE tunnel interface in the dotted decimal format A.B.C.D. The endpoints of the tunnel must be configured by mirroring IP addresses, that is, the tunnel source on one endpoint must be specified as the tunnel destination on the other endpoint.
<interface-name>	Available interface name. Any AlliedWare Plus interface type (eth, ppp, tunnel, lo, etc). Using interface name can minimize the number of user-configured IP addresses and allow the tunnel source IP address to be dynamically issued via, for example, DHCP.

Mode Interface Configuration

Examples To configure a GRE tunnel source IPv4 address, use the commands:

```
awplus# configure terminal
awplus# interface eth1
awplus(config-if)# ip address 1.1.1.1/24
awplus(config-if)# interface tunnel1
awplus(config-if)# tunnel mode gre
awplus(config-if)# tunnel source 1.1.1.1
```

To use an interface name as the tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode gre
awplus(config-if)# tunnel source eth2
```

To remove a GRE tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel source
```

**Related
commands** [interface tunnel \(GRE\)](#)
[tunnel destination \(GRE\)](#)
[tunnel mode gre](#)

tunnel ttl

Overview Use this command to configure the value to use for the Time to Live (TTL) field in the IPv4 header that encapsulates the tunneled IPv4 or IPv6 packets.

Use the **no** variant of this command to set the TTL value to its default.

Syntax `tunnel ttl <1-255>`
`no tunnel ttl`

Parameter	Description
<1-255>	TTL value from 1 through 255.

Default The default TTL value is inherited from the encapsulated packet.

Mode Interface Configuration

Example To set the TTL value of the packet to 255, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel20
awplus(config-if)# tunnel ttl 255
```

To remove the configured TTL value of the packet, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel20
awplus(config-if)# no tunnel ttl
```

Related commands [interface tunnel \(IPv6\)](#)
[interface tunnel \(GRE\)](#)

Introduction

This chapter provides an alphabetical reference of commands used to configure AlliedWare Plus OpenVPN.

For introductory information about AlliedWare Plus OpenVPN, including overview and configuration information, see the [OpenVPN Feature Overview and Configuration_Guide](#).

The table below lists the OpenVPN commands and their applicable modes.

Figure 67-1: OpenVPN commands and applicable modes

Mode	Command
Privileged Exec	<code>show openvpn connections</code>
	<code>show openvpn connections detail</code>
Interface Configuration	<code>tunnel mode openvpn tap</code>
	<code>tunnel mode openvpn tun</code>
	<code>tunnel openvpn port</code>
	<code>tunnel openvpn tagging</code>

- Command List**
- “`ip tcp adjust-mss`” on page 2804
 - “`ipv6 tcp adjust-mss`” on page 2806
 - “`show interface tunnel (OpenVPN)`” on page 2808
 - “`show openvpn connections`” on page 2809
 - “`show openvpn connections detail`” on page 2810
 - “`tunnel mode openvpn tap`” on page 2811
 - “`tunnel mode openvpn tun`” on page 2812

- [“tunnel openvpn authentication”](#) on page 2813
- [“tunnel openvpn cipher”](#) on page 2814
- [“tunnel openvpn expiry-bytes”](#) on page 2816
- [“tunnel openvpn expiry-seconds”](#) on page 2817
- [“tunnel openvpn port”](#) on page 2818
- [“tunnel openvpn route”](#) on page 2819
- [“tunnel openvpn tagging”](#) on page 2821
- [“tunnel openvpn tls-crypt”](#) on page 2822
- [“tunnel openvpn tls-version-min”](#) on page 2823
- [“tunnel openvpn verify-client-certificate trustpoint”](#) on page 2824
- [“tunnel openvpn verify-client-certificate strict-common-name-check”](#) on page 2825
- [“tunnel security-reprocessing”](#) on page 2827

ip tcp adjust-mss

Overview Use this command to set the Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

Syntax `ip tcp adjust-mss {<mss-size>|pmtu}`
`no ip tcp adjust-mss`

Parameter	Description
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	Adjust TCP MSS automatically with respect to the MTU on the interface.

Default The default setting allows a TCP server or a TCP client to set the MSS value for itself.

Mode Interface Configuration

Usage notes When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel

Examples To configure an MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip tcp adjust-mss 1452
```


To configure an MSS size of 1452 bytes on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ip tcp adjust-mss 1452
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip tcp adjust-mss
```

**Related
commands**

[mtu \(PPP\)](#)
[show interface](#)
[show interface \(PPP\)](#)

**Command
changes**

Version 5.4.8-2.1: interface tunnel example added

ipv6 tcp adjust-mss

Overview Use this command to set the IPv6 Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

Syntax `ipv6 tcp adjust-mss {<mss-size>|pmtu}`
`no ipv6 tcp adjust-mss`

Parameter	Description
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	Adjust TCP MSS automatically with respect to the MTU on the interface.

Default The default setting allows a TCP server or a TCP client to set the MSS value for itself.

Mode Interface Configuration

Usage notes When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel

Examples To configure an IPv6 MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To configure an IPv6 MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To adjust IPv6 TCP MSS automatically with respect to the MTU on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ipv6 tcp adjust-mss pmtu
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 tcp adjust-mss
```

**Related
commands**

[mtu \(PPP\)](#)
[show interface](#)
[show interface \(PPP\)](#)
[show interface tunnel \(GRE\)](#)

**Command
changes**

Version 5.4.8-2.1: interface tunnel example added

show interface tunnel (OpenVPN)

Overview Use this command to display status information of a tunnel.

The tunnel remains inactive if no valid tunnel source or tunnel destination is configured.

Syntax `show interface tunnel<tunnel-index>`

Parameter	Description
<tunnel-index>	The tunnel index in the range from 0 to 65535.

Mode Privileged Exec

Examples To display brief status information for OpenVPN tunnel0, enter the command below:

```
awplus# show interface tunnel0
```

Output Figure 67-2: Example output from the **show interface tunnel** command

```
awplus#show interface tunnel0
Interface tunnel0
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 10.8.1.2/24 broadcast 10.8.1.255
  IPv6 address fc00:5::2/64
  IPv6 address fe80::5054:98ff:fe43:428e/64
  index 22 metric 1 mtu 1405
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Tunnel protocol/transport openvpn tap, listen port 1194
  cipher aes128, authentication sha1
  expiry-kbytes 0, expiry-seconds 3600
  tls-version-min 1.0
  Checksumming of packets disabled, DF bit set, path MTU discovery disabled
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
  input packets 0, bytes 0, dropped 0, multicast packets 0
  output packets 6, bytes 452, multicast packets 0, broadcast packets 0
  input average rate : 30 seconds 0 bps, 5 minutes 0 bps
  output average rate: 30 seconds 73 bps, 5 minutes 11 bps
  output peak rate 482 bps at 2021/03/08 01:29:01
  Time since last state change: 0 days 00:00:41
```

Command changes Version 5.5.0-2.1: command added to AR1050V

show openvpn connections

Overview Use this command to show information about connected OpenVPN users.

Syntax `show openvpn connections`

Mode Privileged Exec

Examples To show information about connected OpenVPN users, use the command:

```
awplus# show openvpn connections
```

Output Figure 67-3: Example output from the **show openvpn connections** command

```
awplus#show openvpn connections

Maximum connections: 100

Interface: tunnel0

Username      Real Address      Rx      Tx
              Bytes    Bytes    Connected Since
-----
foo           ::ffff:192.168.1.2 3553    3906    Wed Aug 13 01:09:07 2014
```

Related commands [show openvpn connections detail](#)

Command changes Version 5.5.0-2.1: command added to AR1050V

show openvpn connections detail

Overview Use this command to show detailed information about connected OpenVPN users.

Note that in the output, parameters (such as Route, Address, DNS Server) for a specific user may vary because the parameters depend on the configuration information of the RADIUS server associated with the user.

Syntax `show openvpn connections detail`

Mode Privileged Exec

Examples To show detailed information about connected OpenVPN users, use the command:

```
awplus# show openvpn connections detail
```

Output Figure 67-4: Example output from the **show openvpn connections detail** command

```
awplus#show openvpn connections detail

Interface: tunnel0
Username: user1
Route:      192.168.20.0 255.255.255.0 192.168.10.2
Address:     192.168.10.3 255.255.255.0
DNS Server: 192.168.10.253
DNS Server: 192.168.10.254
VID:        20
Username: user2
Route:      192.168.20.0 255.255.255.0 192.168.10.2
Address:     192.168.10.4 255.255.255.0
DNS Server: 192.168.10.253
DNS Server: 192.168.10.254
VID:        20
```

Related commands [show openvpn connections](#)

Command changes Version 5.5.0-2.1: command added to AR1050V

tunnel mode openvpn tap

Overview Use this command to set the tunnel mode to OpenVPN TAP for a tunnel interface.

Use the **no** variant of this command to remove the mode.

TAP is a virtual network device. TAP creates a Virtual Tunnel Interface (VTI) that carries layer 2 frames. You may want to use TAP in the following scenarios:

- You want to use bridges to transport Ethernet frames
- You want to transport any network protocol, such as IPv4, IPv6, IPX

Note that TAP will cause broadcast overhead on the VPN tunnel and add the overhead of Ethernet headers on all packets transported over the VPN tunnel.

Note that the distribution of client IP addresses through DHCP is only supported in TAP mode.

Syntax `tunnel mode openvpn tap`
`no tunnel mode`

Mode Interface Configuration

Examples To set tunnel5 to be an OpenVPN tunnel in TAP mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# tunnel mode openvpn tap
```

To remove the configured mode for tunnel5, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# no tunnel mode
```

Related commands [tunnel mode openvpn tun](#)

Command changes Version 5.5.0-2.1: command added to AR1050V

tunnel mode openvpn tun

Overview Use this command to set the tunnel mode to OpenVPN TUN for a tunnel interface.

Use the **no** variant of this command to remove the mode.

TUN is a virtual network device. TUN creates a Virtual Tunnel Interface (VTI) that carries layer 3 packets. You may want to use TUN in the following scenarios:

- You want to transport traffic that is destined for the VPN client
- You want to transport only layer 3 packets
- You want to support VPN on mobile devices

Note that TUN cannot be used in bridges and broadcast traffic is not transported in TUN mode.

Syntax `tunnel mode openvpn tun`
`no tunnel mode`

Mode Interface Configuration

Examples To set tunnel5 to be an OpenVPN tunnel in TUN mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# tunnel mode openvpn tun
```

To remove the configured mode for tunnel5, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# no tunnel mode
```

Related commands [tunnel mode openvpn tap](#)

Command changes Version 5.5.0-2.1: command added to AR1050V

tunnel openvpn authentication

Overview Use this command to configure the data channel authentication digest for an OpenVPN tunnel.

Use the **no** variant of this command to set the data channel authentication digest for an OpenVPN tunnel to its default value of SHA1.

Syntax `tunnel openvpn authentication {sha1|sha256}`
`no tunnel openvpn authentication`

Parameter	Description
sha1	Use Secure Hash Standard with 160-bit digest size as the data channel authentication digest.
sha256	Use Secure Hash Standard with 256-bit digest size as the data channel authentication digest.

Default SHA1

Mode Interface configuration

Usage notes You need to configure the client to use the same setting as the server. To do this, include one of the following lines in your client's OpenVPN configuration (.ovpn) file:

Setting	Line
SHA1	auth SHA1
SHA256	auth SHA256

Example To configure tunnel 5, which is an OpenVPN tunnel, to use SHA256 data channel authentication, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# tunnel openvpn authentication SHA256
```

Related commands [tunnel openvpn cipher](#)

Command changes Version 5.4.7-0.1: command added
Version 5.5.0-2.1: command added to AR1050V

tunnel openvpn cipher

Overview Use this command to configure the data channel encryption cipher for an OpenVPN tunnel.

Use the **no** variant of this command to set the data channel encryption cipher for an OpenVPN tunnel to its default value of AES-128.

Syntax tunnel openvpn cipher {aes128|aes256}
no tunnel openvpn cipher

Parameter	Description
aes128	Use Advanced Encryption Standard symmetric key block cipher with a 128-bit key as the data channel encryption cipher.
aes256	Use Advanced Encryption Standard symmetric key block cipher with a 256-bit key as the data channel encryption cipher.

Default AES-128

Mode Interface configuration

Usage notes You need to configure the client to use the same setting as the server. To do this, include one of the following lines in your client's OpenVPN configuration (.ovpn) file:

Setting	Line
AES-128	cipher AES-128-CBC
AES-256	cipher AES-256-CBC

For example, consider a client file tun.ovpn that has the following settings:

```
# tun.ovpn
client
auth-user-pass
cipher AES-128-CBC
dev tap
proto udp
remote 192.168.1.1
ca c:/users/support/cacert.pem
verb 7
```

To change the client to AES-256, replace the line "cipher AES-128-CBC" with "cipher AES-256-CBC".

Example To configure tunnel 5, which is an OpenVPN tunnel, to use AES-256 data channel encryption, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# tunnel openvpn cipher aes256
```

Related commands [tunnel openvpn authentication](#)

Command changes Version 5.4.7-0.1: command added
Version 5.5.0-2.1: command added to AR1050V

tunnel openvpn expiry-bytes

Overview Use this command to change how the firewall decides when to renegotiate client keys. By default, client keys are renegotiated after an hour; you can use this command to base rekeying on data usage instead of time.

Use the **no** variant of this command to return to time-based rekeying instead.

Syntax `tunnel openvpn expiry-bytes <0-4294967295>`
`no tunnel openvpn expiry-bytes`

Parameter	Description
<code>expiry-bytes</code> <code><0-4294967295></code>	The number of bytes of traffic after which the firewall renegotiates client keys. A value of 0 bytes means that keys are not renegotiated after the VPN is formed. Otherwise, setting the expiry-bytes to a non-zero value will cause a rekey when the firewall has received that many bytes of traffic.

Default Not configured - the firewall renegotiates keys every hour instead.

Mode Interface mode for a tunnel

Usage notes If you intend to use more than 100 concurrent tunnels, we recommend you use this command to change to rekeying based on data usage per VPN tunnel instead of timer-based rekeying. Each VPN tunnel will then independently rekey once it reaches the data limit. This prevents all tunnels from rekeying at the same time.

Example To configure tunnel2 to rekey after 1 GB of traffic, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel openvpn expiry-bytes 1000000000
```

To return tunnel2 to the default of rekeying hourly, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel openvpn expiry-bytes
```

Related commands [tunnel openvpn expiry-seconds](#)

Command changes Version 5.4.7-0.1: command added
Version 5.5.0-2.1: command added to AR1050V

tunnel openvpn expiry-seconds

Overview Use this command to change when client keys are renegotiated. By default, client keys are renegotiated after an hour; you can use this command to turn off renegotiation or to change that time period.

Use the **no** variant of this command to return to the default of 1 hour.

Syntax `tunnel openvpn expiry-seconds <0-4294967295>`
`no tunnel openvpn expiry-seconds`

Parameter	Description
<code>expiry-seconds</code> <code><0-4294967295></code>	The length of time after which the firewall renegotiates client keys. A value of 0 seconds means that keys are not renegotiated after the VPN is formed. Otherwise, setting the expiry-seconds to a non-zero timer value will cause a rekey when that time is exceeded.

Default 3600 seconds (1 hour).

Mode Interface mode for a tunnel

Usage notes If you intend to use more than 100 concurrent tunnels, we recommend you change to rekeying based on data usage per VPN tunnel instead of timer-based rekeying. Each VPN tunnel will then independently rekey once it reaches the data limit. This prevents all tunnels from rekeying at the same time. To rekey based on data usage per VPN, use the [tunnel openvpn expiry-bytes](#) command.

Example To configure tunnel2 to rekey every 30 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel openvpn expiry-seconds 1800
```

To return tunnel2 to the default of rekeying hourly, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel openvpn expiry-seconds
```

Related commands [tunnel openvpn expiry-bytes](#)

Command changes Version 5.4.7-0.1: command added
Version 5.5.0-2.1: command added to AR1050V

tunnel openvpn port

Overview Use this command to specify the UDP listening port that is used to receive OpenVPN tunnel connections.

Use the **no** variant to set the port number to its default value which is 1194.

Syntax tunnel openvpn port <1-65535>
no tunnel openvpn port

Parameter	Description
<1-65535>	Port number from 1 through 65535.

Default The default UDP port number is 1194.

Mode Interface Configuration

Usage notes If firewall protection is enabled, you need to create a firewall rule that allows the OpenVPN application traffic to traverse the firewall. OpenVPN is a pre-defined application with destination port number 1194. You can use the [show application detail](#) command to see the application details. If you specify a UDP number that is different to the default port number, you need to create an application with the same specified UDP port number for OpenVPN, and then create a firewall rule to allow the application to traverse the firewall. For more information about firewall rules, see the [rule \(firewall\)](#) command.

Examples To configure tunnel tunnel5 to receive incoming tunnel connections on UDP port 4567, use the commands:

```
awplus(config)# interface tunnel5  
awplus(config-if)# tunnel openvpn port 4567
```

To remove the specified UDP port for tunnel tunnel5 and set the UDP port to its default value, use the commands:

```
awplus# configure terminal  
awplus(config)# interface tunnel5  
awplus(config-if)# no tunnel openvpn port
```

Command changes Version 5.5.0-2.1: command added to AR1050V

tunnel openvpn route

Overview Use this command to push route information based on an entity as part of the OpenVPN client configuration.

When an OpenVPN client connects, the IPv4 and IPv6 host addresses and network subnets for that entity are pushed to the client. This ensures that the client routes those addresses and subnets through the OpenVPN tunnel to the AlliedWare Plus device.

Use the **no** variant of this command to stop pushing the entity as routes to OpenVPN clients.

Syntax `tunnel openvpn route <entity>`
`no tunnel openvpn route`

Parameter	Description
<code><entity></code>	Name of entity containing subnets and addresses to be routed to the device.

Mode Interface Configuration

- Usage notes**
- The gateway IP used will be a configured IP of the OpenVPN tunnel. Host addresses will be sent as /32 IPv4 routes or /128 IPv6 routes.
 - If the network subnets and host IPs change on the entity, client connections will not be automatically updated. Clients will need to reconnect to receive the new routes.
 - Entity network subnets with a configured interface will not be used, as the interface restriction is not applicable for the OpenVPN client in this context.

Example To set up a specific part of the network with certain IP ranges and addresses that will be sent to the OpenVPN client, and ensure that the OpenVPN client directs traffic for these IP ranges to the correct device, use the following commands.

```
awplus# configure terminal
awplus(config)# zone openvpn_routes
awplus(config-zone)# network internet
awplus(config-network)# host example
awplus(config-host)# ip address dynamic fqdn example.com
awplus(config-host)# exit
awplus(config-network)# exit
awplus(config-zone)# network local
awplus(config-network)# ip subnet 172.16.0.0/16
awplus(config-network)# host example
awplus(config-host)# ip address 10.255.0.1
awplus(config-host)# exit
awplus(config-network)# exit
awplus(config-zone)# exit
awplus(config)# interface tunnel1
awplus(config-if)# tunnel openvpn route openvpn_routes
```

To stop pushing an entity as routes to OpenVPN clients, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel openvpn route
```

Related commands [tunnel mode openvpn tap](#)
[tunnel mode openvpn tun](#)

Command changes Version 5.5.4-0.1: command added

tunnel openvpn tagging

Overview This command configures an OpenVPN tunnel to add an 802.1Q tag (a VLAN ID) to traffic received over the tunnel. VLAN ID (VID) is a VLAN identifier that is used to determine which VLAN the traffic belongs to. The VID is determined from information received from the RADIUS server during the authentication process. If no VID information is received from the RADIUS server, the value specified in this command is used.

Use the **no** variant of this command to remove the VID over the tunnel.

Note that you can add an 802.1Q tag in the TAP mode only.

Syntax tunnel openvpn tagging <1-4094>
no tunnel openvpn tagging

Parameter	Description
<1-4094>	VLAN ID from 1 through 4094

Mode Interface Configuration

Examples To add an 802.1Q tag of 1 to packets received over the tunnel named tunnel5, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# tunnel openvpn tagging 1
```

To remove the 802.1Q tag for the tunnel named tunnel5, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel5
awplus(config-if)# no tunnel openvpn tagging
```

Command changes Version 5.5.0-2.1: command added to AR1050V

tunnel openvpn tls-crypt

Overview Use this command to enable TLS Crypt on OpenVPN. TLS Crypt uses a pre-shared key to secure the entire OpenVPN session from the first packet. It provides several potential benefits:

- It prevents detection of the OpenVPN connection start, which is helpful in some situations when the OpenVPN protocol signature is detected and blocked.
- It prevents TLS denial of service attacks. DoS attacks are possible with TLS-Auth, where the attacker can open thousands of TLS connections simultaneously but not provide a valid certificate, jamming the available ports. With TLS Crypt the server would reject the connection up front.
- Data is encrypted twice, once by TLS Crypt and once by the TLS session.

Use the **no** variant of this command to disable TLS Crypt.

Syntax `tunnel openvpn tls-crypt <key-filename>`
`no tunnel openvpn tls-crypt`

Parameter	Description
<code><key-filename></code>	The path to the key file that is shared with the clients. The filename starts with "flash:/" (e.g. flash:/openvpn.key). All clients and the server must share the same key file. TLS Crypt will automatically create the configured key file if it doesn't exist.

Default Disabled

Mode Interface Configuration for a tunnel

Example To configure OpenVPN in TAP mode, and use the key file called 'openvpn.key' on tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel openvpn tls-crypt flash:/openvpn.key
awplus(config-if)# tunnel mode openvpn tap
```

Related commands [tunnel mode openvpn tap](#)
[tunnel mode openvpn tun](#)

Command changes Version 5.5.2-0.1: command added

tunnel openvpn tls-version-min

Overview Use this command to set the minimum TLS (Transport Layer Security) version allowed for OpenVPN.

Use the **no** variant of this command to revert to the default TLS version (1.0).

Syntax `tunnel openvpn tls-version-min {1.1|1.2|1.3}`
`no tunnel openvpn tls-version-min`

Parameter	Description
tls-version-min	Enter the minimum TLS version: 1.1, 1.2, or 1.3. If the command is never entered, or the 'no' version is configured, then the default version 1.0 is used.

Default 1.0

Mode Interface Configuration

Example To set the minimum TLS version as 1.1 on Open VPN tunnel1, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# tunnel openvpn tls-version-min 1.1
```

Related commands [tunnel openvpn cipher](#)
[tunnel openvpn expiry-bytes](#)

Command changes Version 5.5.1-2.1: TLS version 1.3 added
Version 5.5.1-0.1: command added

tunnel openvpn verify-client-certificate trustpoint

Overview Use this command to enable OpenVPN to check a certificate provided by the client when they try to connect. This is a form of Two-Factor Authentication (2FA) called mutual trust. The certificate provided by the client, and the certificate owned by the server, must both be signed by the same certificate authority (CA).

Use the **no** variant of this command to disable the trustpoint.

Syntax `tunnel openvpn verify-client-certificate trustpoint
<trustpoint-name>`
`no tunnel openvpn verify-client-certificate trustpoint
<trustpoint-name>`

Parameter	Description
<code><trustpoint-name></code>	The name of the trustpoint which contains the required certificates. For example, 'openvpn_selfsigned'.

Default Disabled

Mode Interface Configuration

Usage notes The trustpoint part of the command allows the user to configure which certificates the server will be checking the client against. This is only available on the Interface Configuration for a tunnel.

Examples To enable this feature on 'tunnel1' and use the trustpoint called 'openvpn_selfsigned', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# tunnel openvpn verify-client-certificate
trustpoint openvpn_selfsigned
```

To disable this feature on 'tunnel1', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel openvpn verify-client-certificate
trustpoint openvpn_selfsigned
```

Related commands [tunnel openvpn verify-client-certificate strict-common-name-check](#)

Command changes Version 5.5.3-0.1: command added

tunnel openvpn verify-client-certificate strict-common-name-check

Overview Use this command to provide a valid certificate and check that the common name on the certificate matches the client's username.

Use the **no** variant of this command to remove the strict common name check.

Syntax

```
tunnel openvpn verify-client-certificate
strict-common-name-check

no tunnel openvpn verify-client-certificate
strict-common-name-check
```

Parameter	Description
strict-common-name-check	The valid certificate common name. This name must match the client's user name.

Default The strict common name check is enabled by default.

Mode Interface Configuration

Usage notes The strict common name check part of this command allows the user to provide a method for client certificate authentication for the OpenVPN server along with the username and password.

Example To disable this feature on 'tunnel1', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel openvpn verify-client-certificate
strict-common-name-check
```

To require OpenVPN clients to provide a valid certificate and check that the common name on the certificate matches the client's username, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# tunnel openvpn verify-client-certificate
strict-common-name-check
```

Output Figure 67-5: Example output from **tunnel openvpn verify-client-certificate**

```
awplus(config-if)#tunnel openvpn verify-client-certificate
strict-common-name-check

Strict name check is enabled
```

Related commands [tunnel openvpn verify-client-certificate trustpoint](#)

Command changes Version 5.5.3-0.1: command added

tunnel security-reprocessing

Overview Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

Syntax `tunnel security-reprocessing`
`no tunnel security-reprocessing`

Default Security reprocessing is disabled by default.

Mode Global Configuration

Usage notes Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#).

Example To enable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# no tunnel security-reprocessing
```

Related commands [show interface tunnel \(GRE\)](#)
[show interface tunnel \(IPsec\)](#)
[show interface tunnel \(L2TPv3\)](#)
[show interface tunnel \(OpenVPN\)](#)

Command changes Version 5.4.8-0.2: command added

68

L2TPv3 Ethernet Pseudowire Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure L2TPv3 Ethernet pseudowires.

For introductory information about L2TPv3 in AlliedWare Plus, including overview and configuration information, see the [L2TPv3 Ethernet Pseudowire Feature Overview and Configuration Guide](#).

- Command List**
- “[interface tunnel \(L2TPv3\)](#)” on page 2829
 - “[l2tp unmanaged port](#)” on page 2830
 - “[show interface tunnel \(L2TPv3\)](#)” on page 2831
 - “[tunnel destination \(L2TPv3\)](#)” on page 2832
 - “[tunnel df](#)” on page 2834
 - “[tunnel local id](#)” on page 2835
 - “[tunnel mode l2tp v3](#)” on page 2836
 - “[tunnel protection ipsec](#)” on page 2837
 - “[tunnel remote id](#)” on page 2838
 - “[tunnel security-reprocessing](#)” on page 2839
 - “[tunnel source \(L2TPv3\)](#)” on page 2840

interface tunnel (L2TPv3)

Overview Use this command to create a tunnel interface or to enter Interface mode to configure an existing tunnel. Tunnel interfaces are identified by an index identifier that is an integer in the range from 0 through 65535.

Use the **no** variant of this command to remove a previously created tunnel interface.

Syntax `interface tunnel<0-65535>`
`no interface tunnel<tunnel-index>`

Parameter	Description
<0-65535>	Specify a tunnel interface index identifier in the range from 0 through 65535.

Default Tunnel interfaces do not exist.

Mode Global Configuration

Usage notes After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

Examples To configure a tunnel interface with index 30 and enable L2TPv3 mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel30
awplus(config-if)# tunnel mode l2tp v3
```

To remove the tunnel interface tunnel30, use the commands:

```
awplus# configure terminal
awplus(config)# no interface tunnel30
```

Related commands [show interface tunnel \(L2TPv3\)](#)
[tunnel mode l2tp v3](#)

Command changes Version 5.4.7-2.1: increased range for **tunnel** index identifiers.

l2tp unmanaged port

Overview Use this command to set the UDP port for an (IPv4 and IPv6) unmanaged L2TP tunnel (L2TPv3 Ethernet Pseudowires).

This command can only change the UDP port when there is no unmanaged L2TP tunnel (L2TPv3 Ethernet Pseudowires) configured.

Use the **no** variant of this command to reset the UDP port to the default (1701).

Syntax `l2tp unmanaged port [<1-65535>]`
`no l2tp unmanaged port`

Parameter	Description
<1-65535>	The number of the UDP port to use for an unmanaged L2TP tunnel (L2TPv3 Ethernet Pseudowires).

Default The UDP port is 1701 by default.

Mode Global Configuration

Usage notes The default UDP port for both unmanaged and managed L2TP tunnels is 1701. If both kinds of tunnel will be configured, the UDP port for the unmanaged tunnel must be changed to a different port by using the **l2tp unmanaged port** command.

Be aware of potential clashes with other UDP port users. Unless it is likely to be used for other purposes, we recommend configuring UDP port 1702 as a suitable alternative.

Example To set the UDP port for an L2TP unmanaged tunnel (L2TPv3 Ethernet Pseudowires) to 1702, use the following commands:

```
awplus# configure terminal
awplus(config)# l2tp unmanaged port 1702
```

Related commands [tunnel mode l2tp v3](#)
[show running-config](#)

show interface tunnel (L2TPv3)

Overview Use this command to display status information of a tunnel.

Syntax show interface tunnel<0-65535>

Parameter	Description
<0-65535>	Specify a tunnel index in the range from 0 through 65535.

Mode Privileged Exec

Examples To display status information for L2TPv3 tunnel tunnel20, use the command.

```
awplus#show interface tunnel20
```

Output Figure 68-1: Example output from **show tunnel interface** on the console.

```
awplus#show interface tunnel20
Interface tunnel20
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 192.168.10.1/24 broadcast 192.168.10.255
  IPv6 address 2001:db8:10::1/64
  IPv6 address fe80::5054:d4ff:fe84:d1aa/64
  index 16795714 metric 1 mtu 1480
  arp ageing timeout 300
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Tunnel source 192.168.1.1, destination 192.168.1.2
  Tunnel name local 192.168.1.1, remote 192.168.1.2
  Tunnel ID local 66, remote 77
  Tunnel protocol/transport l2tp v3, key disabled, sequencing
  disabled
  Tunnel TTL inherit
  Checksumming of packets disabled, path MTU discovery disabled
  input packets 0, bytes 0, dropped 0, multicast packets 0
  output packets 5, bytes 366, multicast packets 0 broadcast
  packets 0
  Time since last state change: 0 days 00:00:24
```

Related commands [interface tunnel \(L2TPv3\)](#)

tunnel destination (L2TPv3)

Overview Use this command to specify a tunnel destination for the remote end of the tunnel. Tunnel destination can be specified by using a destination network name or an IPv4 address.

Use the **no** variant of this command to remove a configured tunnel destination.

Syntax `tunnel destination {<ipv4-addr>|<destination-network-name>}`
`no tunnel destination`

Parameter	Description
<code><ipv4-addr></code>	Specify the tunnel destination IPv4 address in the dotted decimal format A.B.C.D. The endpoints of the tunnel must be configured by mirroring IP addresses, that is, the tunnel source on one endpoint must be specified as the tunnel destination on the other endpoint.
<code><destination-network-name></code>	Destination network name. If the destination network name cannot be resolved, then the L2TPv3 tunnel remains inactive.

Mode Interface Configuration

Examples To configure an IPv4 tunnel destination by using an IPv4 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel destination 2.2.2.2
```

To configure an L2TPv3 tunnel destination by using a destination network name, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel destination
corporate_lan.example.com
```

To remove a tunnel destination, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# no tunnel destination
```

Related commands interface tunnel (L2TPv3)
 tunnel mode l2tp v3
 tunnel source (L2TPv3)

tunnel df

Overview Use this command to specify whether the DF (Don't Fragment) bit in the IP header should be set or not on outgoing packets from L2TPv3 tunnels.

Use the **no** variant of this command to return to the default setting.

Syntax `tunnel df {set|clear}`
`no tunnel df`

Parameter	Description
set	Set the DF bit in the outer header
clear	Clear the DF bit in the outer header

Default The DF bit is **set** on all outgoing packets.

Mode Interface Configuration

Usage notes This command gives you the opportunity to clear the DF bit allowing packets greater than the MTU to be fragmented and transmitted via the L2TPv3 Ethernet pseudo-wire. This may be necessary if an L2TPv3 tunnel is connected to a bridge and MTU-exceeded messages cannot be sent back to clients.

NOTE: If fragmentation of larger packets occurs as a result of setting the tunnel Do Not Fragment bit to clear, this may slightly increase latency of the associated traffic flow traversing the VPN, due to the fragmentation and re-assembly that occurs.

Example To specify the DF bit on the L2TPv3 tunnel (tunnel2), use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel df clear
```

To set the DF bit on the L2TPv3 tunnel (tunnel2) back to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel df
```

Related commands [tunnel mode l2tp v3](#)

Command changes Version 5.4.9-1.1: command added

tunnel local id

Overview This command specifies a tunnel local identifier sent to the peer to match.
Use the **no** variant of this command to remove the tunnel local ID.

Syntax `tunnel local id <1-2147483647>`
`no tunnel local id`

Parameter	Description
<1-2147483647>	Tunnel ID from 1 through 2147483647

Default No tunnel local ID is set.

Mode Interface Configuration

Usage notes The endpoints of the tunnel must be configured by mirroring tunnel IDs, that is, the tunnel local ID on one endpoint must be specified as the tunnel remote ID on the other endpoint.

The local session ID defaults to the tunnel local ID and the local session ID is not configurable. A session provides the data channel in L2TPv3. There is a single pseudowire per L2TP session.

Examples To specify a tunnel local ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#tunnel mode l2tp v3
awplus(config-if)#tunnel local id 22
```

To remove the tunnel local ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#no tunnel local id
```

Related commands [tunnel remote id](#)

Validation Commands [show interface tunnel \(L2TPv3\)](#)

tunnel mode l2tp v3

Overview Use this command to configure the encapsulation tunneling mode.
Use the **no** variant of this command to remove an established tunnel.

Syntax `tunnel mode l2tp v3 [ipv6]`
`no tunnel mode`

Parameter	Description
ipv6	Specify IPv6 as the delivery protocol.

Default Virtual tunnel interfaces have no mode set by default. If you specify a mode of **l2tp v3**, the delivery protocol is IPv4 unless you specify IPv6.

Mode Interface Configuration

Usage notes A tunnel will not become operational until it is configured with this command.

Examples To configure L2TPv3 as the encapsulation tunneling mode for tunnel20, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#tunnel mode l2tp v3
```

To remove the established tunnel20, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#no tunnel mode
```

Related commands [interface tunnel \(L2TPv3\)](#)
[show interface tunnel \(L2TPv3\)](#)
[tunnel df](#)

tunnel protection ipsec

Overview Use this command to optionally enable IPsec protection for packets encapsulated by this tunnel.

Use the **no** variant of this command to disable IPsec protection.

Syntax `tunnel protection ipsec [profile <ipsec-profile>]`
`no tunnel protection ipsec`

Parameter	Description
<ipsec-profile>	The name of an optional custom IPsec profile (crypto ipsec profile command) to use to protect this tunnel.

Default IPsec protection for packets encapsulated by tunnel is disabled.

Mode Interface Configuration

Usage notes You also need to configure a pre-shared key in conjunction with this command. See the [crypto isakmp key](#) command for more information about configuring the pre-shared key.

Examples To enable IPsec protection for packets encapsulated by tunnel114, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel114
awplus(config-if)#tunnel protection ipsec
```

To disable IPsec protection for packets encapsulated by tunnel114, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel114
awplus(config-if)#no tunnel protection ipsec
```

Related commands [crypto ipsec profile](#)
[crypto isakmp key](#)
[show isakmp key \(IPsec\)](#)

tunnel remote id

Overview This command specifies a tunnel remote identifier sent to the peer for match.
Use the **no** variant of this command to remove the tunnel remote ID.

Syntax tunnel remote id <1-2147483647>
no tunnel remote id

Parameter	Description
<1-2147483647>	Tunnel ID from 1 through 2147483647

Default No tunnel remote ID is set.

Mode Interface Configuration

Usage notes The endpoints of the tunnel must be configured by mirroring tunnel IDs, that is, the tunnel remote ID on one endpoint must be specified as the tunnel local ID on the other endpoint.

The remote session ID defaults to the tunnel remote ID and the remote session ID is not configurable. A session provides the data channel in L2TPv3. There is a single pseudowire per L2TP session.

Examples To specify a tunnel remote ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#tunnel mode l2tp v3
awplus(config-if)#tunnel remote id 22
```

To remove the tunnel remote ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#no tunnel remote id
```

Related commands [tunnel local id](#)

Validation Commands [show interface tunnel \(L2TPv3\)](#)

tunnel security-reprocessing

Overview Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

Syntax `tunnel security-reprocessing`
`no tunnel security-reprocessing`

Default Security reprocessing is disabled by default.

Mode Global Configuration

Usage notes Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#).

Example To enable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# no tunnel security-reprocessing
```

Related commands [show interface tunnel \(GRE\)](#)
[show interface tunnel \(IPsec\)](#)
[show interface tunnel \(L2TPv3\)](#)
[show interface tunnel \(OpenVPN\)](#)

Command changes Version 5.4.8-0.2: command added

tunnel source (L2TPv3)

Overview Use this command to specify a tunnel source for the tunnel interface. The tunnel source can be specified by using an interface name or an IPv4 address. The source address must be an existing IPv4 address configured for an interface.

Use the **no** variant of this command to remove a tunnel source for a tunnel interface.

Syntax tunnel source {<ipv4-addr>|<interface-name>}
no tunnel source

Parameter	Description
<ipv4-addr>	Specify the tunnel source IPv4 address for the tunnel interface in the dotted decimal format A.B.C.D. The endpoints of the tunnel must be configured by mirroring IP addresses, that is, the tunnel source on one endpoint must be specified as the tunnel destination on the other endpoint.
<interface-name>	Available interface name. Any AlliedWare Plus interface type (eth, ppp, tunnel, lo, etc). Using interface name can minimize the number of user-configured IP addresses and allow the tunnel source IP address to be dynamically issued via, for example, DHCP.

Mode Interface Configuration

Examples To configure an L2TPv3 tunnel source IPv4 address, use the commands:

```
awplus# configure terminal
awplus# interface eth0
awplus(config-if)# ip address 1.1.1.1/24
awplus(config-if)# interface tunnel1
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel source 1.1.1.1
```

To use an interface name as the tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel source eth2
```

To remove a tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel source
```

Related commands

- [interface tunnel \(L2TPv3\)](#)
- [tunnel destination \(L2TPv3\)](#)
- [tunnel mode l2tp v3](#)

69

Transitioning IPv4 to IPv6 Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure Light Weight 4 over 6 and MAP E.

Many ISPs have migrated from IPv4 to IPv6 networks. However, many customers are still using IPv4 facilities. IPv6 transition technologies, such as Light Weight 4 over 6 (LW4o6) and MAP-E, provide interoperability between IPv4 and IPv6 networks. This enables ISPs with IPv6 networks to provide Internet connectivity to customers with IPv4 facilities.

MAP-E provides a mechanism for mapping between an IPv4 prefix or IPv4 address or IPv4 shared address and an IPv6 address. It also uses the encapsulation mode described in RFC 2473 (IPv6 Tunneling) to transport IPv4 packets over an IPv6 network.

Dual-Stack Lite (DS-Lite) (RFC 6333) describes an architecture for transporting IPv4 packets over an IPv6 network. This chapter describes an extension to DS-Lite called **Lightweight 4over6**, which moves the Network Address and Port Translation (NAPT) function from the centralized DS-Lite tunnel concentrator to the tunnel client located in the Customer Premises Equipment (CPE).

This removes the requirement for a Carrier Grade NAT function in the tunnel concentrator and reduces the amount of centralized state that must be held to a per-subscriber level. In order to delegate the NAPT function and make IPv4 address sharing possible, port-restricted IPv4 addresses are allocated to the CPEs.

- Useful Terms**
- **Softwire:** A tunnel between two IPv6 end-points to carry IPv4 packets or two IPv4 end-points to carry IPv6 packets.
 - **B4:** Softwire at the customer end that encapsulates native packets and tunnels them to a softwire concentrator (AFTR) at the service provider.
 - **AFTR:** Softwire that decapsulates the packets received from a softwire B4 and sends them to their destination.

For more information, see the [Transitioning IPv4 to IPv6 Feature Overview and Configuration Guide](#).

- Command List**
- ["4to6-mapping"](#) on page 2844
 - ["br-address \(softwire\)"](#) on page 2845
 - ["clear 4to6-mapping"](#) on page 2846
 - ["ip dns forwarding dns46"](#) on page 2848
 - ["ip dns forwarding dns64"](#) on page 2850
 - ["limits \(4to6-mapping\)"](#) on page 2851
 - ["map4to6 \(4to6-mapping\)"](#) on page 2852
 - ["map6to4 \(4to6-mapping\)"](#) on page 2854
 - ["mesh-mode"](#) on page 2856
 - ["method"](#) on page 2857
 - ["originator \(4to6-mapping\) \(deprecated\)"](#) on page 2858
 - ["responder \(4to6-mapping\) \(deprecated\)"](#) on page 2859
 - ["rule"](#) on page 2860
 - ["show 4to6-mapping"](#) on page 2862
 - ["show ip dns forwarding dns46"](#) on page 2863
 - ["show running-config softwire-configuration"](#) on page 2864
 - ["show softwire-configuration"](#) on page 2865
 - ["softwire-configuration"](#) on page 2867
 - ["tunnel destination \(DS-Lite\)"](#) on page 2868
 - ["tunnel mode ds-lite"](#) on page 2869
 - ["tunnel mode lw4o6"](#) on page 2870
 - ["tunnel mode map-e"](#) on page 2871
 - ["tunnel security-reprocessing"](#) on page 2872
 - ["tunnel softwire"](#) on page 2873
 - ["upstream-interface"](#) on page 2874

4to6-mapping

Overview Use this command to add an IPv4 to IPv6 address mapping set and enter the IPv4 to IPv6 Address Mapping Configuration mode.

Use the **no** variant of this command to remove an IPv4 to IPv6 address mapping set.

Syntax 4to6-mapping <name>
no 4to6-mapping <name>

Parameter	Description
<name>	The name of the 4to6 mapping.

Mode Global Configuration

Usage notes In some computer networks, there are two separate networks that need to be connected together, but one network only has IPv4 and one only has IPv6. This mapping configuration allows you to specify mappings between the address ranges for use with transition technologies to connect those networks together.

Example To add an IPv4 to IPv6 address mapping set named 'test' and enter IPv4 to IPv6 Address Mapping Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)#
```

To remove an IPv4 to IPv6 address mapping set named 'test', use the commands:

```
awplus# configure terminal
awplus(config)# no 4to6-mapping test
```

Related commands [clear 4to6-mapping](#)
[limits \(4to6-mapping\)](#)
[map4to6 \(4to6-mapping\)](#)
[show 4to6-mapping](#)

Command changes Version 5.5.0-2.0: command added

br-address (software)

Overview Use this command to specify the IPv6 address of the MAP-E Border Router. Note, before using this command you must configure the command **method (Software Configuration)** with the **static** parameter.

Use the **no** variant of this command to remove the MAP-E Border Router address configuration.

Syntax `br-address <ipv6-address>`
`no br-address`

Parameter	Description
<code><ipv6-address></code>	IPv6 address of MAP-E Border Router

Default Not set.

Mode SoftWire Configuration

Example To configure 'swconfig' to the software configuration MAP-E Border Router IPv6 address, use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# br-address 2001::1
```

To remove the MAP-E Border Router IPv6 address configuration for 'swconfig', use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# no br-address
```

Related commands [show software-configuration](#)

Command changes Version 5.4.9-0.1: command added

clear 4to6-mapping

Overview Use this command to clear one, some, or all of the IPv4 to IPv6 address mappings that were automatically created by the DNS46 system.

This command runs in 3 modes:

- **all** - removes all entries installed by the specified system
- **exact** - removes an exact match
- **non-exact** - removes all entries that are contained by both the IPv4 and IPv6 subnets provided

Syntax

```
clear 4to6-mapping <name> responder all dns46  
clear 4to6-mapping <name> responder exact <ipv4-address>  
<ipv6-address>  
clear 4to6-mapping <name> responder [exact] <ipv4-subnet>  
<ipv6-prefix>
```

Parameter	Description
<name>	The 4to6 mapping group name.
all	Remove all entries created by the specified system.
exact	Require an exact match on the IPv4 and IPv6 addresses or subnets.
<ipv4-address>	The IPv4 address uses the format A.B.C.D.
<ipv4-subnet>	The IPv4 address uses the format A.B.C.D/M.
<ipv6-address>	
<ipv6-prefix>	

Mode Privileged Exec

Example To remove all entries installed by DNS46 in the 'test' 4 to 6 mapping, use the command:

```
awplus# clear 4to6-mapping test responder all dns46
```

To remove the mapping between 192.0.2.1 and 2001:db8::1, use the command:

```
awplus# clear 4to6-mapping test responder exact 192.0.2.1  
2001:db8::1
```

To remove the mapping between 192.0.2.0/24 and 2001:db8::/120, use the command:

```
awplus# clear 4to6-mapping test responder exact 192.0.2.0/24  
2001:db8::/120
```

To remove any mapping between 192.0.2.2 (with any IPv6 address), use the command:

```
awplus# clear 4to6-mapping test responder 192.0.2.2/32::/0
```

To remove any mapping between 2001:db8::2 (with any IPv4 address), use the command:

```
awplus# clear 4to6-mapping test responder 0.0.0.0  
2001:db8::2/128
```

**Related
commands**

[4to6-mapping](#)
[show 4to6-mapping](#)

**Command
changes**

Version 5.5.0-2.0: command added

ip dns forwarding dns46

Overview Use this command to enable DNS46, which provides 4 to 6 mapping functionality within DNS relay. This feature allows for single IPv4 to IPv6 mappings to a mapping instance, such as NAT46.

Use the **no** variant of this command to disable DNS46 settings.

Syntax

```
ip dns forwarding dns46
ip dns forwarding dns46 <name> [subnet
[<ipv4-address/m>|<ipv6-address/prefix-length>]
no ip dns forwarding dns46
no ip dns forwarding dns46 <name> [subnet
[<ipv4-address/m>|<ipv6-address/prefix-length>]
```

Parameter	Description
<name>	The name of the 4to6 mapping instance.
<ip-address/m>	The IPv4 subnet to operate DNS46 over for the listed mapping instance.
<ipv6-address/prefix-length>	The IPv6 prefix to operate DNS46 over for the listed mapping instance.

Mode Global Configuration

Default DNS46 is disabled by default. DNS46 does not have a default mapping instance. For a set mapping instance, it will operate on all subnets if none are configured.

Usage notes In some computer networks, there may be two separate networks that need to communicate with each other: one with only IPv4 and the other with only IPv6. DNS46 enables DNS A requests to flow from the IPv4 network to the IPv6 network and back. It provides the necessary mappings (from A to AAAA) to the mapping instance (NAT46).

Examples To enable DNS46, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dns46
```

To set the DNS46 mapping instance, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dns46 nat46
```

To add a DNS46 mapping instance's IPv4 subnet to operate over, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dns46 subnet 192.168.1.0/24
```

To add a DNS46 mapping instance's IPv6 subnet to operate over, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dns46 subnet 2001:db8:1::/64
```

To disable DNS46, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46
```

To remove a DNS46 mapping instance, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46 nat46
```

To remove a DNS46 mapping instance's IPv4 subnet to operate over, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46 nat46 subnet
192.168.1.0/24
```

To remove a DNS46 mapping instance's IPv6 subnet to operate over, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46 nat46 subnet
2001:db8:1::/64
```

To remove all a DNS46 mapping instance's subnets, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46 nat46 subnet
```

Output Figure 69-1: Example output from **ip dns forwarding dns46**

```
If you are setting a DNS46 mapping instance but one is already
set, the error and output is as follows:% DNS46 doesn't support
multiple mapping instances

If you are adding a subnet to a dns46 mapping instance but the
listed DNS46 mapping instance doesn't exist it will output:% DNS46
mapping instance '%s' doesn't exist.
```

Related commands [ip dns forwarding](#)
[show 4to6-mapping](#)

Command changes Version 5.5.3-2.1: command added

ip dns forwarding dns64

Overview Use this command to enable DNS64 translation, using the given map4to6 instance.

DNS64 implements DNS query translations between an IPv6 client subnet and IPv6 server subnet. Together with NAT64, this feature supports IPv6 clients in communicating with IPv4 servers by translating the addresses in DNS AAAA records.

When a DNS query is made for an IPv6 address (AAAA record), it will translate the AAAA record into an A record (which contains the IPv4 address).

Use the **no** variant of this command to disable DNS64 translating using the given map4to6 instance.

Syntax `ip dns forwarding dns64 <map4to6-instance>[translate-all]`
`no ip dns forwarding dns64 <map4to6-instance>`

Parameter	Description
<map4to6-instance>	The name of the 4to6 mapping instance.
translate-all	Apply DNS64 translation to all DNS AAAA requests, not just members of the configured 4to6-mapping instance map6to4 rule. This is useful for hosts that contact their local DNS server via link-local addresses.

Default DNS64 is disabled by default and does not have a default mapping instance.

Mode Global Configuration

Example To enable DNS64 with a map4to6 instance, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dns46 nat64
```

To enable DNS64 with a map4to6 instance, and apply DNS64 translation to all DNS AAAA requests, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dns46 nat64 translate-all
```

To disable DNS64, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dns46 nat64
```

Related commands [ip dns forwarding](#)

Command changes Version 5.5.4-1.1: command added

limits (4to6-mapping)

Overview Use this command to limit the dynamic 4to6 mappings created by DNS46. You can limit the maximum number and the maximum age of those dynamic mappings.

Use the **no** variant of this command to remove the configured size and age limits.

Syntax `limits dynamic {size <size-limit>|age <age-limit>}`
`no limits dynamic {size|age}`

Parameter	Description
size	Limit the maximum number of dynamic mappings.
<size-limit>	The limit for the maximum number of dynamic mappings.
age	Limit the maximum age for mappings.
<age-limit>	The limit for the age of unused dynamic mappings in seconds.

Default There are no limits on the maximum number or maximum age of dynamic mappings.

Mode IPv4 to IPv6 Address Mapping Configuration

Example To limit the 4to6 mapping 'test' to a maximum of 500 dynamic mappings with a maximum age of 86400 seconds (24 hours), use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# limits dynamic size 500
awplus(config-4to6-mapping)# limits dynamic age 86400
```

To remove the limits on the 4to6 mapping 'test', use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# no limits dynamic size
awplus(config-4to6-mapping)# no limits dynamic age
```

Related commands [4to6-mapping](#)
[show 4to6-mapping](#)

Command changes Version 5.5.0-1.3: command added

map4to6 (4to6-mapping)

Overview Use this command to specify the IPv4 to IPv6 address mapping.

Use the **no** variant of this command to remove the IPv4 to IPv6 address mapping.

Syntax

```
map4to6 single <ip-address> <ipv6-address> [ipv6-interface <interface>]

map4to6 subnet <ip-address/m> <ipv6-address/prefix-length> [ipv6-interface <interface>]

no map4to6 single <ip-address> <ipv6-address> [ipv6-interface <interface>]

no map4to6 subnet <ip-address/m> <ipv6-address/prefix-length> [ipv6-interface <interface>]
```

Parameter	Description
single	Configure a single IPv4 to IPv6 mapping.
<ip-address>	The IPv4 address to map.
<ipv6-address>	The IPv6 address to map.
subnet	Map an entire subnet between IPv4 and IPv6.
<ip-address/m>	The IPv4 subnet to map.
<ipv6-address/prefix-length>	The IPv6 prefix to map.
ipv6-interface <interface>	Specify the name of the interface to use to determine part of the IPv6 subnet.

Mode IPv4 to IPv6 Address Mapping Configuration

Usage notes There are three supported mapping modes:

- **single** - maps a specific IPv4 address to a specific IPv6 address
- **subnet** - maps an IPv4 subnet into an IPv6 subnet
- **ipv6-interface** - use this mode if you have a dynamic IPv6 subnet assigned (by RA or DHCPv6) and want to use addresses from it.

The network component of the address on that interface will combine with the supplied IPv6 address/subnet and the IPv4 address to produce an IPv6 address. For example, if the interface is assigned 2001:db8:1::/64 and 192.168.1.1 (in single mode), the resulting IPv6 address would be 2001:db8:1::192.168.1.1

Example To map all IPv4 addresses to the IPv6 subnet on eth1 (using zeros for the parts that are not specified by the subnet or IPv4 address), use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# map4to6 subnet 0.0.0.0/0 ::/96
ipv6-interface eth1
```

To remove that mapping, use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# no map4to6 subnet 0.0.0.0/0 ::/96
ipv6-interface eth1
```

Related commands

- [4to6-mapping](#)
- [map6to4 \(4to6-mapping\)](#)
- [show 4to6-mapping](#)

Command changes Version 5.5.3-2.1: command added

map6to4 (4to6-mapping)

Overview Use this command to specify the IPv4 to IPv6 address mapping to use for the responding device (i.e. the destination of the first packet seen).
Use the **no** variant of this command to remove the IPv4 to IPv6 address mapping.

Syntax `map6to4 single <ip-address> <ipv6-address>`
`map6to4 subnet <ip-address/m> <ipv6-address/prefix-length>`
`no map6to4 single <ip-address> <ipv6-address>`
`no map6to4 subnet <ip-address/m> <ipv6-address/prefix-length>`

Parameter	Description
single	Configure a single IPv4 to IPv6 mapping.
<ip-address>	The IPv4 address to map.
<ipv6-address>	The IPv6 address to map.
subnet	Map an entire subnet between IPv4 and IPv6.
<ip-address/m>	The IPv4 subnet to map.
<ipv6-address/prefix-length>	The IPv6 subnet to map.

Mode IPv4 to IPv6 Address Mapping Configuration

Usage notes There are two supported mapping modes:

- **single** - maps a specific IPv4 address to a specific IPv6 address
- **subnet** - maps an IPv4 subnet into an IPv6 prefix. You could map all IPv4 addresses to 64::A.B.C.D by specifying 64::/96.

Example To map the IPv4 address 192.0.2.1 to IPv6 address 2001:db8::1, use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# map6to4 single 192.0.2.1
2001:db8::1
```

To remove the mapping, use the commands:

```
awplus# configure terminal
awplus(config)# 4to6-mapping test
awplus(config-4to6-mapping)# no map6to4 single 192.0.2.1
2001:db8::1
```

Related commands [4to6-mapping](#)
[map4to6 \(4to6-mapping\)](#)

`show 4to6-mapping`

Command changes Version 5.5.3-0.1: command added

mesh-mode

Overview Use this command to enable mesh-mode. Mesh-mode enables software tunnels to work with devices that share the same IP address at the tunnel endpoint.

Use the **no** variant of this command to disable mesh-mode.

Syntax `mesh-mode`
`no mesh-mode`

Default No mesh-mode.

Mode SoftWire Configuration

Usage notes Software tunnels may require communication with endpoints sharing the same IP address. The CPU resource required to support this is significant, so this command enables this support.

Example To configure a software named 'demo' to communicate with endpoints that share the same IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration demo
awplus(config-software)# mesh-mode
```

Related commands [show software-configuration](#)
[software-configuration](#)

Command changes Version 5.4.9-0.1: command added

method

Overview Use this command to specify the configuration method (or source) for a software configuration. The configuration method can be either static or DHCP.

Use the **no** variant of this command to remove a configured method.

Syntax `method {static|dhcp}`
`no method`

Parameter	Description
static	Software configuration is statically configured
dhcp	Software configuration is acquired through DHCP

Default Not set.

Mode SoftWire Configuration

Example To set the 'swconfig' software configuration method to **static**, use the commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# method static
```

To set the 'swconfig' software configuration method to **DHCP**, use the commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# method dhcp
```

To remove the software configuration method from 'swconfig', use the commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# no method
```

Related commands [show software-configuration rule](#)

Command changes Version 5.4.9-0.1: command added

originator (4to6-mapping) (deprecated)

Overview This command has been deprecated in software version 5.5.4-1.1. Use the command [map4to6 \(4to6-mapping\)](#) instead.

responder (4to6-mapping) (deprecated)

Overview This command has been deprecated in software version 5.5.4-1.1. Use the command [map6to4 \(4to6-mapping\)](#) instead.

rule

Overview Use this command to statically configure a MAP rule. Note, before using this command you must configure the command **method (Softwire Configuration)** with the **static** parameter.

You would normally obtain the values to use in this command from your ISP.

Use the **no** variant of this command to remove a MAP rule configuration.

Syntax

```
rule <0-65535> ipv4-prefix <ipv4-prefix> ipv6-prefix
<ipv6-prefix> psid-length <0-15> psid <psid-value> [offset
<0-16>] [forwarding]

rule <0-65535> ipv4-prefix <ipv4-prefix> ipv6-prefix
<ipv6-prefix> ea-length <0-48> [offset <0-16>] [forwarding]

no rule <0-65535>
```

Parameter	Description
rule <0-65535>	Rule ID is an integer in the range <1-65535>
ipv4-prefix <ipv4-prefix>	IPv4 prefix (e.g. 192.0.2.0/24)
ipv6-prefix <ipv6-prefix>	IPv6 prefix (e.g. 2001:db8::/32)
ea-length <0-48>	Embedded address length is an integer in the range <0-48>.
psid-length <0-15>	Port Set ID (PSID) length is an integer in the range <0-15>, the default length is 0.
psid <psid-value>	Port Set ID (PSID) value is either decimal <0-65535> or hexadecimal with a leading 0x. Different PSID values guarantee non-overlapping port sets.
offset <0-16>	Port Set ID (PSID) offset is an integer in the range <0-16>.
forwarding	Indicates if this rule is a Forwarding Mapping Rule (FMR). Otherwise, this is only used as a Basic Mapping Rule (BMR)

Default Not set.

Mode SoftWire Configuration

Example To configure a MAP rule 1 and MAP rule 2 in Software Configuration 'swconfig', use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# rule 1 ipv4-prefix 192.0.2.0/24
ipv6-prefix 2001:db8:1::/48 ea-length 16 forwarding
awplus(config-software)# rule 2 ipv4-prefix 192.0.2.23/32
ipv6-prefix 2001:db8:1:1781::/64 psid-length 8 psid 129
```

These two example rules above produce the same resulting IPv4 address and PSID if the IPv6 subnet on the upstream interface is 2001:db8:1:1781::/64.

To the remove rule 1 in Software Configuration 'swconfig', use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# no rule 1
```

Related commands [method](#)
[show software-configuration](#)

Command changes Version 5.4.9-0.1: command added

show 4to6-mapping

Overview Use this command to show all the IPv4 to IPv6 address mappings the system has. The output of this command includes manually configured mappings and the ones that the DNS46 component generated and installed.

Syntax `show 4to6-mapping`

Mode Privileged Exec

Usage notes Use the **no map4to6** or **no map6to4** commands to remove manually configured individual entries. Use the **clear 4to6-mapping** command to remove DNS46 entries.

Example To show IPv4 to IPv6 mapping instances, use the command:

```
awplus# show 4to6-mapping
```

Output Figure 69-2: Example output from **show 4to6-mapping**

```
awplus#show 4to6-mapping
IPv4 to IPv6 Instances:

Mapping Instance: test
  Originator Mappings:
    user subnet mapping between 0.0.0.0/0 and ::/96 using ipv6
    subnet from eth1
  Responder Mappings:
    user single mapping between 192.0.2.1 and 2001:db8::1
```

Related commands

- [4to6-mapping](#)
- [clear 4to6-mapping](#)
- [map4to6 \(4to6-mapping\)](#)
- [map6to4 \(4to6-mapping\)](#)
- [ip dns forwarding dns46](#)
- [limits \(4to6-mapping\)](#)

Command changes Version 5.5.3-0.1: command added

show ip dns forwarding dns46

Overview Use this command to view the DNS relay DNS46 settings. DNS46 is an IPv4 to IPv6 transitional technology, which is used in conjunction with NAT46.

Syntax `show ip dns forwarding dns46`

Mode User Exec

Example To view the DNS relay DNS46 settings, use the command:

```
awplus# show ip dns forwarding dns46
```

Output Figure 69-3: Example output from **show ip dns forwarding dns46**

```
##This example shows DNS46 is enabled with an instance 'nat46' and some IP subnets.

awplus#show ip dns forwarding dns46

Status      : Enabled
Instance    : nat46
  IPv4 Ranges
    178.15.2.1/24
    10.0.0.0/8
    172.18.0.0/16
  IPv6 Ranges
    f002::f1/16
    fff1::f1/16
```

Related commands [show ip dns forwarding](#)

Command changes Version 5.5.3-2.1: command added

show running-config software-configuration

Overview Use this command to display the running configuration information for a software configuration.

Syntax `show running-config software-configuration`
`<software-config-name>`
`show running-config software-configuration`

Parameter	Description
<code><software-config-name></code>	The name assigned for the Software Configuration

Mode Privileged Exec

Example To show the running configuration for **all** software configuration, use the following command:

```
awplus# show running-config software-configuration
```

To show the running configuration for software configuration 'swconfig1', use the following command:

```
awplus# show running-config software-configuration swconfig1
```

Output Figure 69-4: Example output from **show running-config software-configuration**

```
awplus#show running-config software-configuration
software-configuration swconfig1
  method static
  map-version rfc
  br-address 2001:db8:1234:5678::1
  rule 10 ipv4-prefix 192.168.1.0/24 ipv6-prefix 2001:db8:1000::/48 ea-length 16 forwarding
  rule 20 ipv4-prefix 192.168.2.0/24 ipv6-prefix 2001:db8:2000::/48 ea-length 16 forwarding
  rule 30 ipv4-prefix 192.168.3.0/24 ipv6-prefix 2001:db8:3000::/48 ea-length 16 forwarding
!
software-configuration swconfig2
  method dhcp
  upstream-interface eth1
!
```

Related commands [software-configuration](#)

Command changes Version 5.4.9-0.1: command added

show software-configuration

Overview Use this command to show information about the configuration state of software configuration. You can show information for all software configurations or define a specific configuration for display.

Syntax `show software-configuration <software-config-name>`
`show software-configuration`

Parameter	Description
<code><software-config-name></code>	Name assigned to the Software Configuration

Mode Privileged Exec

Example To show information about the configuration state of **all** software configuration, use the command:

```
awplus# show software-configuration
```

To show information about the configuration state of software configuration 'swconfig1', use the command:

```
awplus# show software-configuration swconfig1
```

Output Figure 69-5: Example output for a Static MAP-E software configuration

```
awplus#show software-configuration swconfig1

Software Configuration: swconfig1

Configuration Source: static
Upstream Interface: eth1
MAP-E Version: rfc
No LW4o6 Configuration

Border Relay Device: 2001:db8::1
Rule 0
  IPv4-prefix: 192.0.2.0/24
  IPv6-prefix: 2001:db8::/32
  Embedded address length: 16
  Forwarding: enabled
  PSID offset: default
  PSID length: default
  PSID: default (0x0)
```

Figure 69-6: Example output for LW4o6 (config method DHCP)

```
awplus#show software-configuration

Software Configuration: lw4o6

Configuration Source: dhcp
Upstream Interface: eth1
MAP-E Version: rfc
lwAFTR Address: 2001:0db8:acc3:0055:0000:0000:0000:0001
lw4o6 Rule:
  IPv4-Address: 192.0.2.123
  IPv6-Prefix: 2001:0db8::/32
  PSID offset: 0
  PSID length: 9
  PSID: 346 (0x15a)

Border Relay Device: Not Set
```

**Related
commands**

[software-configuration
method
br-address \(software\)
upstream-interface
rule](#)

**Command
changes**

Version 5.4.9-0.1: command added

software-configuration

Overview Use this command to enter the Software Configuration mode. This mode allows you to configure software settings.

In computer networking, a software is a type of tunneling protocol that creates a virtual "wire" that transparently encapsulates another protocol. Softwares are used for various purposes, one of which is to carry IPv4 traffic over IPv6 and vice versa, in order to support IPv6 transition mechanisms.

Use the **no** variant of this command to remove a software configuration.

Syntax `software-configuration <software-config-name>`
`no software-configuration <software-config-name>`

Parameter	Description
<code><software-config-name></code>	The name assigned for this software configuration

Mode Global Configuration

Example To configure software settings for 'software1', use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration software1
awplus(config-software)#
```

To remove software 'software1', MAP Rules configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# no software-configuration software1
```

Related commands [show software-configuration](#)

Command changes Version 5.4.9-0.1: command added

tunnel destination (DS-Lite)

Overview Use this command to specify the tunnel destination for a DS-Lite tunnel.
Use the **no** variant of this command to remove a configured tunnel destination.

Syntax `tunnel destination dhcp interface <interface-name>`
`no tunnel destination`

Parameter	Description
<code><interface-name></code>	The interface which receives the DHCP reply.

Mode Interface Configuration

Example To configure a DS-Lite tunnel destination, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel mode ds-lite
awplus(config-if)# tunnel destination dhcp interface eth1
```

To remove the tunnel destination, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# no tunnel mode destination
```

Related commands [tunnel mode ds-lite](#)

Command changes Version 5.4.9-0.1: command added

tunnel mode ds-lite

Overview Use this command to set the tunnel mode to DS-Lite for a tunnel interface.

Use the **no** variant of this command to remove the tunnel mode.

Syntax tunnel mode ds-lite
no tunnel mode

Default Not set.

Mode Interface Configuration

Example To configure the DS-Lite tunnel mode on interface 'tunnel0', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel mode ds-lite
```

To remove the configured DS-Lite tunnel mode for 'tunnel0', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# no tunnel mode
```

Related commands [tunnel mode \(IPv6\)](#)

Command changes Version 5.4.9-0.1: command added

tunnel mode lw4o6

Overview Use this command to set the tunnel mode to Light Weight 4over6 (lw4o6) for a tunnel interface.

Use the **no** variant of this command to remove an established lw4o6 tunnel.

Syntax `tunnel mode lw4o6`
`no tunnel mode`

Default Not set.

Mode Interface Configuration

Example To configure lw4o6 tunnel mode for tunnel6, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel mode lw4o6
```

To removed the configured lw4o6 tunnel mode for tunnel6, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel mode
```

Related commands [tunnel mode \(IPv6\)](#)

Command changes Version 5.4.9-0.1: command added

tunnel mode map-e

Overview Use this command to set the tunnel mode to MAP-E for a tunnel interface.
Use the **no** variant of this command to remove the MAP-E mode from a tunnel interface.

Syntax tunnel mode map-e
no tunnel mode

Default Not set.

Mode User Exec and Privileged Exec

Example To configure the MAP-E tunnel mode on interface 'tunnel6', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel mode map-e
```

To remove the configured MAP-E tunnel mode for 'tunnel6', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel mode
```

Related commands [show software-configuration](#)

Command changes Version 5.4.9-0.1: command added

tunnel security-reprocessing

Overview Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

Syntax `tunnel security-reprocessing`
`no tunnel security-reprocessing`

Default Security reprocessing is disabled by default.

Mode Global Configuration

Usage notes Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the [Internet Protocol Security \(IPsec\) Feature Overview and Configuration Guide](#).

Example To enable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# no tunnel security-reprocessing
```

Related commands [show interface tunnel \(GRE\)](#)
[show interface tunnel \(IPsec\)](#)
[show interface tunnel \(L2TPv3\)](#)
[show interface tunnel \(OpenVPN\)](#)

Command changes Version 5.4.8-0.2: command added

tunnel software

- Overview** Use this command to configure the software configuration to use for a tunnel interface.
- Note that **tunnel-mode map-e** or **tunnel mode lw4o6** must be configured in order for the command **tunnel software** to be valid.
- Use the **no** variant of this command to remove a tunnel software configuration.

Syntax `tunnel software <software-config-name>`
`no tunnel software`

Parameter	Description
<code><software-config-name></code>	The software configuration used for a tunnel interface

Default Not set.

Mode Interface Configuration

Example To set the software configuration called 'swconfig' to an interface called 'tunnel6', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel software swconfig
```

To remove the software configuration for interface 'tunnel6', use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel software
```

Related commands [tunnel mode map-e](#)
[tunnel mode lw4o6](#)

Command changes Version 5.4.9-0.1: command added

upstream-interface

Overview Use this command to assign a softwire configuration to an upstream interface configured with a globally scoped IPv6 address.

Use the **no** variant of this command to remove a configured upstream interface.

Syntax `upstream-interface <interface-name>`
`no upstream-interface`

Parameter	Description
<code><interface-name></code>	Name of the interface connected to upstream (e.g. eth1, br1, vlan1)

Default Not set.

Mode SoftWire Configuration

Example To configure the softwire configuration ('swconfig') upstream-interface to eth1, use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# upstream-interface eth1
```

To remove the softwire configuration ('swconfig') upstream-interface configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# software-configuration swconfig
awplus(config-software)# no upstream-interface
```

Related commands [show software-configuration](#)

Command changes Version 5.4.9-0.1: command added

70

IPv6 Tunneling Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure IPv6 Tunneling.

For more information, see the [IPv6 Tunneling Feature Overview and Configuration Guide](#).

- Command List**
- ["interface tunnel \(IPv6\)"](#) on page 2876
 - ["ip address \(IP Addressing and Protocol\)"](#) on page 2877
 - ["ip tcp adjust-mss"](#) on page 2879
 - ["ipv6 address"](#) on page 2881
 - ["ipv6 tcp adjust-mss"](#) on page 2883
 - ["mtu"](#) on page 2885
 - ["show interface tunnel \(IPv6\)"](#) on page 2887
 - ["tunnel destination \(IPv6\)"](#) on page 2888
 - ["tunnel dscp"](#) on page 2890
 - ["tunnel mode \(IPv6\)"](#) on page 2891
 - ["tunnel source \(IPv6\)"](#) on page 2892
 - ["tunnel ttl"](#) on page 2894

interface tunnel (IPv6)

Overview Use this command to create a tunnel interface or to enter Interface mode to configure an existing tunnel. Tunnel interfaces are identified by an index identifier that is an integer in the range from 0 through 65535.

Use the **no** variant of this command to remove a previously created tunnel interface.

Syntax `interface tunnel< tunnel-index>`
`no interface tunnel< tunnel-index>`

Parameter	Description
< tunnel-index>	Specify a tunnel interface index identifier in the range from 0 through 65535.

Default Tunnel interfaces do not exist.

Mode Global Configuration

Usage notes After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

Examples To configure a tunnel interface with index 30 and use IPv6 tunneling, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel30
awplus(config-if)# tunnel mode ipv6
```

To remove the IPv6 tunnel interface tunnel30, use the commands:

```
awplus# configure terminal
awplus(config)# no interface tunnel30
```

Command changes Version 5.4.8-2.1: command added

ip address (IP Addressing and Protocol)

Overview This command sets a static IP address on an interface.

The **no** variant of this command removes the IP address from the interface.

You cannot remove the primary address when a secondary address is present.

Syntax `ip address <ip-addr/prefix-length> [secondary] [label <label>]`
`no ip address [<ip-addr/prefix-length>] [secondary]`

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length you are assigning to the interface.
secondary	Secondary IP address.
label	Adds a user-defined description of the secondary IP address.
<label>	A user-defined description of the secondary IP address. Valid characters are any printable character and spaces.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes To set the primary IP address on the interface, specify only **ip address** <ip-addr/prefix-length>. This overwrites any configured primary IP address. To add additional IP addresses on this interface, use the **secondary** parameter. You must configure a primary address on the interface before configuring a secondary address.

NOTE: Use **show running-config interface**, instead of **show ip interface brief**, when you need to view a secondary address configured on an interface. **show ip interface brief** will only show the primary address, not a secondary address for an interface.

Examples To add the IP address 10.10.10.50/24 to the interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip address 10.10.10.50/24
```

To add the secondary IP address 10.10.11.50/24 to the same interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip address 10.10.11.50/24 secondary
```

To add the IP address 10.10.11.50/24 to the local loopback interface lo, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the PPP interface ppp0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the tunnel tunnel0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# ip address 10.10.11.50/24
```

**Related
commands**

[interface \(to configure\)](#)
[show ip interface](#)
[show running-config interface](#)

ip tcp adjust-mss

Overview Use this command to set the Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

Syntax `ip tcp adjust-mss {<mss-size>|pmtu}`
`no ip tcp adjust-mss`

Parameter	Description
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	Adjust TCP MSS automatically with respect to the MTU on the interface.

Default The default setting allows a TCP server or a TCP client to set the MSS value for itself.

Mode Interface Configuration

Usage notes When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel

Examples To configure an MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ip tcp adjust-mss 1452
```

To configure an MSS size of 1452 bytes on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ip tcp adjust-mss 1452
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ip tcp adjust-mss
```

**Related
commands**

[mtu \(PPP\)](#)
[show interface](#)
[show interface \(PPP\)](#)

**Command
changes**

Version 5.4.8-2.1: interface tunnel example added

ipv6 address

Overview Use this command to set the IPv6 address of an interface. The command also enables IPv6 on the interface, which creates an EUI-64 link-local address as well as enabling RA processing and SLAAC.

To stop the device from processing prefix information (routes and addresses from the received Router Advertisements) use the command **no ipv6 nd accept-ra-pinfo**.

To remove the EUI-64 link-local address, use the command **no ipv6 eui64-linklocal**.

Use the **no** variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

Syntax `ipv6 address <ipv6-addr/prefix-length>`
`no ipv6 address <ipv6-addr/prefix-length>`

Parameter	Description
<code><ipv6-addr/prefix-length></code>	Specifies the IPv6 address to be set. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a PPP interface, a bridge, or a tunnel.

Usage notes Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them. See the [ipv6 enable](#) command for more information.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the [ipv6 enable](#) command then it will not be removed using a **no ipv6 address** command.

Examples To assign the IPv6 address 2001:0db8::a2/64 to eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

To assign the IPv6 address to the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To assign the IPv6 address to the tunnel tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

**Related
commands**

[ipv6 address autoconfig](#)

[ipv6 address dhcp](#)

[ipv6 dhcp server](#)

[ipv6 enable](#)

[ipv6 eui64-linklocal](#)

[show running-config](#)

[show ipv6 interface](#)

[show ipv6 route](#)

ipv6 tcp adjust-mss

Overview Use this command to set the IPv6 Maximum Segment Size (MSS) size for an interface, where MSS is the maximum TCP data packet size that the interface can transmit before fragmentation.

Use the **no** variant of this command to remove a previously specified MSS size for a PPP interface, and restore the default MSS size.

Syntax `ipv6 tcp adjust-mss {<mss-size>|pmtu}`
`no ipv6 tcp adjust-mss`

Parameter	Description
<mss-size>	<64-1460> Specifies the MSS size in bytes.
pmtu	Adjust TCP MSS automatically with respect to the MTU on the interface.

Default The default setting allows a TCP server or a TCP client to set the MSS value for itself.

Mode Interface Configuration

Usage notes When a host initiates a TCP session with a server it negotiates the IP segment size by using the MSS option field in the TCP packet. The value of the MSS option field is determined by the Maximum Transmission Unit (MTU) configuration on the host.

You can set a feasible MSS value on the following interfaces:

- PPP
- Ethernet
- Tunnel

Examples To configure an IPv6 MSS size of 1452 bytes on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To configure an IPv6 MSS size of 1452 bytes on Ethernet interface eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# ipv6 tcp adjust-mss 1452
```

To adjust IPv6 TCP MSS automatically with respect to the MTU on interface tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# ipv6 tcp adjust-mss pmtu
```

To restore the MSS size to the default size on PPP interface ppp0, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 tcp adjust-mss
```

**Related
commands**

[mtu \(PPP\)](#)
[show interface](#)
[show interface \(PPP\)](#)
[show interface tunnel \(GRE\)](#)

**Command
changes**

Version 5.4.8-2.1: interface tunnel example added

mtu

Overview Use this command to set the Maximum Transmission Unit (MTU) size for interfaces, where MTU is the maximum packet size that interfaces can transmit. The MTU size setting is applied to both IPv4 and IPv6 packet transmission.

Use the **no** variant of this command to remove a previously specified Maximum Transmission Unit (MTU) size, and restore the default MTU size. For example, the eth interface default is 1500 bytes.

Syntax `mtu <68-1582>`
`no mtu`

Parameter	Description
<code><68-1582></code>	The Maximum Transmission size in bytes.

Default The default MTU size, for example 1500 bytes for eth interfaces.

Mode Interface Configuration

Usage notes If a device receives an IPv4 packet for Layer 3 switching to another interface with an MTU size smaller than the packet size, and if the packet has the '**don't fragment**' bit set, then the device will send an ICMP '**destination unreachable**' (3) packet type and a '**fragmentation needed and DF set**' (4) code back to the source. For IPv6 packets bigger than the MTU size of the transmitting interface, an ICMP '**packet too big**' (ICMP type 2 code 0) message is sent to the source.

You can set a feasible MTU value on the following interfaces:

- PPP
- Ethernet
- Tunnel

Note that you cannot configure MTU on bridge interfaces. The MTU of the bridge interface is determined by the member interface of the bridge which has the lowest MTU. For example, if you attach eth0 with MTU 1200 and tunnel1 with MTU 1500 to a bridge interface, the MTU for that interface will be 1200.

Examples To configure an MTU size of 1555 bytes for tunnel 'tunnel2', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# mtu 1555
```

Related commands [show interface](#)

- Command changes** Version 5.4.7-1.1: Behavior change when MTU set to less than 1500 on FS980M and GS980M.
- Version 5.5.1-0.1: Layer 3 jumbo frames supported on SBx908 GEN2 and x950.
- Version 5.5.1-1.2: Layer 3 jumbo frames supported on x530 and GS980MX.

show interface tunnel (IPv6)

Overview Use this command to display status information of tunnels.

The tunnel remains inactive if no valid tunnel source or tunnel destination is configured.

Syntax `show interface tunnel< tunnel-index>`

Parameter	Description
tunnel	Specify this parameter to display tunnel status information of a given tunnel identified by the <0-255> parameter.
<0-255>	Specify a tunnel index in the range from 0 through 255.

Mode Privileged Exec

Example To display status information for IPv6 tunnel tunnel20, use the command:

```
awplus# show interface tunnel20
```

Figure 70-1: Example output from the **show interface tunnel** command

```
awplus#show interface tunnel20
Interface tunnel20
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 192.168.10.1/24 pointopoint 192.168.10.255
  index 4751 metric 1 mtu 1480
  arp ageing timeout 300
  <UP,POINTOPOINT,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Tunnel source 2001:db8::1:1, destination 2001:db8::2:1
  Tunnel name local 2001:db8::1:1, remote 2001:db8::2:1
  Tunnel ID local (not set), remote (not set)
  Tunnel protocol/transport ipv6, key disabled, sequencing disabled
  Tunnel TTL 64
  Checksumming of packets disabled, path MTU discovery disabled
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 22:38:35
```

Command changes Version 5.4.8-2.1: command added

tunnel destination (IPv6)

Overview Use this command to specify a tunnel destination for the remote end of the tunnel. Tunnel destination can be specified by using a destination network name or an IPv6 address.

Use the **no** variant of this command to remove a configured tunnel destination.

Syntax `tunnel destination {<ipv6-addr>|<destination-network-name>}`
`no tunnel destination`

Parameter	Description
<code><ipv6-addr></code>	Specify the tunnel destination IPv6 address in the dotted decimal format x:x::x:x. The endpoints of the tunnel must be configured by mirroring IP addresses, that is, the tunnel source on one endpoint must be specified as the tunnel destination on the other endpoint.
<code><destination-network-name></code>	Destination network name. If the destination network name cannot be resolved, then the IPv6 tunnel remains inactive.

Mode Interface Configuration

Examples To configure an IPv6 tunnel destination by using an IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode ipv6
awplus(config-if)# tunnel destination 2001:db8::1:1
```

To configure an IPv6 tunnel destination by using a destination network name, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode ipv6
awplus(config-if)# tunnel destination
corporate_lan.example.com
```

To remove a IPv6 tunnel destination, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# no tunnel destination
```

Related commands [interface tunnel \(IPv6\)](#)

tunnel mode (IPv6)

tunnel source (IPv6)

Command changes Version 5.4.8-2.1: command added

tunnel dscp

Overview Use this command to configure the Differentiated Services Code Point (DSCP) value for the DSCP field in the packet header that encapsulates the tunneled packets.

Use the **no** variant of this command to reset the DSCP field to its default value.

Syntax `tunnel dscp <0-63>`
`no tunnel dscp`

Parameter	Description
<0-63>	Specify the DSCP value in the range from 0 through 63 for the DSCP field in the packet header that encapsulates the tunneled packets.

Default The IPv4 DSCP field value is inherited from the inner header to the outer header.

Mode Interface Configuration

Examples To configure the DSCP value to 10 for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel dscp 10
```

To remove a configured DSCP value for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel dscp
```

Related commands [interface tunnel \(IPv6\)](#)
[interface tunnel \(GRE\)](#)

tunnel mode (IPv6)

Overview Use this command to configure the encapsulation tunneling mode to use. This command sets IPv6 tunneling.

Use the **no** variant of this command to remove an established tunnel.

Syntax `tunnel mode ipv6`
`no tunnel mode`

Default Virtual tunnel interfaces have no mode set by default.

Mode Interface Configuration

Usage notes A tunnel will not become operational until it is configured with this command.

Examples To configure IPv6 as the encapsulation mode for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode ipv6
```

To remove a configured IPv6 tunnel mode for tunnel2, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel mode
```

Related commands [interface tunnel \(IPv6\)](#)

Command changes Version 5.4.8-2.1: command added

tunnel source (IPv6)

Overview Use this command to specify a tunnel source for the tunnel interface. Tunnel source can be specified by using an interface name or an IPv6 address. The source address must be an existing IPv6 address configured for an interface.

Use the **no** variant of this command to remove a tunnel source for a tunnel interface.

Syntax tunnel source {<ipv6-addr>|<interface-name>}
no tunnel source

Parameter	Description
<ipv6-addr>	Specify the tunnel source IPv6 address for the IPv6 tunnel interface in the dotted decimal format x:x::x:x. The endpoints of the tunnel must be configured by mirroring IP addresses, that is, the tunnel source on one endpoint must be specified as the tunnel destination on the other endpoint.
<interface-name>	Available interface name. Any AlliedWare Plus interface type (eth, ppp, tunnel, lo, etc). Using interface name can minimize the number of user-configured IP addresses and allow the tunnel source IP address to be dynamically issued via, for example, DHCP.

Mode Interface Configuration

Examples To configure an IPv6 tunnel source IPv6 address, use the commands:

```
awplus# configure terminal
awplus# interface eth1
awplus(config-if)# ip address 2001:db8::1:1/48
awplus(config-if)# interface tunnel1
awplus(config-if)# tunnel mode ipv6
awplus(config-if)# tunnel source 2001:db8::1:1
```

To use an interface name as the tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode ipv6
awplus(config-if)# tunnel source eth1
```

To remove an IPv6 tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel source
```


Related commands interface tunnel (IPv6)
 tunnel destination (IPv6)
 tunnel mode (IPv6)

Command changes Version 5.4.8-2.1: command added

tunnel ttl

Overview Use this command to configure the value to use for the Time to Live (TTL) field in the IPv4 header that encapsulates the tunneled IPv4 or IPv6 packets.

Use the **no** variant of this command to set the TTL value to its default.

Syntax `tunnel ttl <1-255>`
`no tunnel ttl`

Parameter	Description
<1-255>	TTL value from 1 through 255.

Default The default TTL value is inherited from the encapsulated packet.

Mode Interface Configuration

Example To set the TTL value of the packet to 255, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel20
awplus(config-if)# tunnel ttl 255
```

To remove the configured TTL value of the packet, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel20
awplus(config-if)# no tunnel ttl
```

Related commands [interface tunnel \(IPv6\)](#)
[interface tunnel \(GRE\)](#)