

IE200 Series

INDUSTRIAL MANAGED PoE+ SWITCHES

AT-IE200-6FT-80

AT-IE200-6FP-80

AT-IE200-6GT-80

AT-IE200-6GP-80



Command Reference for AlliedWare Plus™ Version 5.4.5

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 ©1998-2008 The OpenSSL Project. All rights reserved.

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/default.aspx

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, and VCStack are trademarks or registered trademarks in the United States and elsewhere of Allied Telesis, Inc.

Adobe, Acrobat, and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries. Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. Netscape Navigator is a registered trademark of Netscape Communications Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

© 2015 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

Chapter 1:	CLI Navigation Commands	52
	Introduction	52
	configure terminal	53
	disable (Privileged Exec mode)	54
	do	55
	enable (Privileged Exec mode)	56
	end	58
	exit	59
	help	60
	logout	61
	show history	62
Chapter 2:	User Access Commands	63
	Introduction	63
	clear line console	65
	clear line vty	66
	enable password	67
	enable secret	70
	exec-timeout	73
	flowcontrol hardware (asyn/console)	75
	length (asyn)	77
	line	78
	privilege level	80
	security-password history	81
	security-password forced-change	82
	security-password lifetime	83
	security-password minimum-categories	84
	security-password minimum-length	85
	security-password reject-expired-pwd	86
	security-password warning	87
	service advanced-vty	88

service password-encryption	.89
service telnet	.90
service terminal-length (deleted)	.91
show privilege	.92
show security-password configuration	.93
show security-password user	.94
show telnet	.95
show users	.96
telnet	.97
telnet server	.98
terminal length	.99
terminal resize	100
username	101

Chapter 3: File Management Commands 103

Introduction	103
autoboot enable	107
boot config-file	108
boot config-file backup	110
boot system	111
boot system backup	113
cd	114
copy current-software	115
copy debug	116
copy running-config	117
copy startup-config	118
copy (filename)	119
copy zmodem	121
create autoboot	122
delete	123
delete debug	124
dir	125
edit	127
edit (filename)	128
erase startup-config	130
mkdir	131
move	132
move debug	133
pwd	134
rmdir	135
show autoboot	136
show boot	137
show file	139
show file systems	140
show running-config	142
show running-config access-list	144
show running-config dhcp	145
show running-config full	146
show running-config interface	147
show running-config ipv6 access-list	149
show running-config key chain	150
show running-config lldp	151
show running-config power-inline	152

show running-config router-id	153
show running-config security-password	154
show startup-config	155
show version	156
write file	157
write memory	158
write terminal	159

Chapter 4: System Configuration and Monitoring Commands 160

Introduction	160
banner exec	162
banner login (system)	164
banner motd	166
clock set	168
clock summer-time date	169
clock summer-time recurring	171
clock timezone	173
continuous-reboot-prevention	174
ecofriendly led	176
findme	177
hostname	178
no debug all	180
reboot	181
reload	182
show clock	183
show continuous-reboot-prevention	185
show cpu	186
show cpu history	189
show debugging	192
show ecofriendly	193
show interface memory	194
show memory	196
show memory allocations	198
show memory history	200
show memory pools	201
show memory shared	202
show process	203
show reboot history	205
show router-id	206
show system	207
show system environment	208
show system interrupts	209
show system mac	210
show system pluggable	211
show system pluggable detail	213
show system pluggable diagnostics	217
show system serialnumber	219
show tech-support	220
speed (asyn)	222
system territory (deprecated)	224
terminal monitor	225
undebg all	226

Chapter 5:	Logging Commands	227
	Introduction	227
	clear exception log	229
	clear log	230
	clear log buffered	231
	clear log permanent	232
	default log buffered	233
	default log console	234
	default log email	235
	default log host	236
	default log monitor	237
	default log permanent	238
	log buffered	239
	log buffered (filter)	240
	log buffered size	243
	log console	244
	log console (filter)	245
	log email	248
	log email (filter)	249
	log email time	252
	log host	254
	log host (filter)	255
	log host time	258
	log monitor (filter)	260
	log permanent	263
	log permanent (filter)	264
	log permanent size	267
	log-rate-limit nsm	268
	show counter log	270
	show exception log	271
	show log	272
	show log config	275
	show log permanent	278
	show running-config log	279
 Chapter 6:	 Scripting Commands	 280
	Introduction	280
	activate	281
	echo	282
	wait	283
 Chapter 7:	 Interface Commands	 284
	Introduction	284
	description (interface)	285
	interface (to configure)	286
	mru jumbo	288
	mtu	289
	show interface	291
	show interface brief	294
	show interface status	295
	shutdown	297

Chapter 8:	Interface Testing Commands	298
	Introduction	298
	clear test interface	299
	service test	300
	test interface	301
Chapter 9:	Alarm Monitoring Commands	303
	Introduction	303
	alarm facility	304
	show alarm settings	307
	show facility-alarm status	308
Chapter 10:	Switching Commands	309
	Introduction	309
	backpressure	311
	clear loop-protection counters	313
	clear mac address-table static	314
	clear mac address-table dynamic	315
	clear port counter	317
	debug loopprot	318
	debug platform packet	319
	duplex	321
	flowcontrol (switch port)	322
	linkflap action	324
	loop-protection	325
	loop-protection action	326
	loop-protection action-delay-time	327
	loop-protection timeout	328
	mac address-table acquire	329
	mac address-table ageing-time	330
	mac address-table static	331
	mirror interface	332
	platform stop-unreg-mc-flooding	334
	platform vlan-stacking-tpid	336
	polarity	337
	show debugging loopprot	338
	show debugging platform packet	339
	show flowcontrol interface	340
	show interface err-disabled	341
	show interface switchport	342
	show loop-protection	343
	show mac address-table	344
	show mirror	346
	show mirror interface	347
	show platform	348
	show platform classifier statistics utilization brief	349
	show platform port	350
	speed	354
	undebg loopprot	356
	undebg platform packet	357
Chapter 11:	VLAN Commands	358

Introduction	358
port-vlan-forwarding-priority	360
private-vlan	363
private-vlan association	364
show port-vlan-forwarding-priority	365
show vlan	366
show vlan classifier group	367
show vlan classifier group interface	368
show vlan classifier interface group	369
show vlan classifier rule	370
show vlan private-vlan	371
switchport access vlan	372
switchport enable vlan	373
switchport mode access	374
switchport mode private-vlan	375
switchport mode private-vlan trunk promiscuous	376
switchport mode private-vlan trunk secondary	378
switchport mode trunk	380
switchport private-vlan host-association	381
switchport private-vlan mapping	382
switchport trunk allowed vlan	383
switchport trunk native vlan	386
switchport vlan-stacking (double tagging)	388
switchport voice dscp	389
switchport voice vlan	390
switchport voice vlan priority	392
vlan	393
vlan classifier activate	394
vlan classifier group	395
vlan classifier rule ipv4	396
vlan classifier rule proto	397
vlan database	400

Chapter 12: Spanning Tree Commands 401

Introduction	401
clear spanning-tree statistics	403
clear spanning-tree detected protocols (RSTP and MSTP)	404
debug mstp (RSTP and STP)	405
instance priority (MSTP)	409
instance vlan (MSTP)	411
region (MSTP)	413
revision (MSTP)	414
show debugging mstp	415
show spanning-tree	416
show spanning-tree brief	419
show spanning-tree mst	420
show spanning-tree mst config	421
show spanning-tree mst detail	422
show spanning-tree mst detail interface	424
show spanning-tree mst instance	426
show spanning-tree mst instance interface	427
show spanning-tree mst interface	428
show spanning-tree mst detail interface	429

show spanning-tree statistics	431
show spanning-tree statistics instance	433
show spanning-tree statistics instance interface	435
show spanning-tree statistics interface	437
show spanning-tree vlan range-index	440
spanning-tree autoedge (RSTP and MSTP)	441
spanning-tree bpdu	442
spanning-tree cisco-interoperability (MSTP)	444
spanning-tree edgeport (RSTP and MSTP)	445
spanning-tree enable	446
spanning-tree errdisable-timeout enable	448
spanning-tree errdisable-timeout interval	449
spanning-tree force-version	450
spanning-tree forward-time	451
spanning-tree guard root	452
spanning-tree hello-time	453
spanning-tree link-type	454
spanning-tree max-age	455
spanning-tree max-hops (MSTP)	456
spanning-tree mode	457
spanning-tree mst configuration	458
spanning-tree mst instance	459
spanning-tree mst instance path-cost	460
spanning-tree mst instance priority	462
spanning-tree mst instance restricted-role	463
spanning-tree mst instance restricted-tcn	464
spanning-tree path-cost	466
spanning-tree portfast (STP)	467
spanning-tree portfast bpdu-filter	469
spanning-tree portfast bpdu-guard	471
spanning-tree priority (bridge priority)	473
spanning-tree priority (port priority)	474
spanning-tree restricted-role	475
spanning-tree restricted-tcn	476
spanning-tree transmit-holdcount	477
undebg mstp	478

Chapter 13: Link Aggregation Commands 479

Introduction	479
channel-group	481
clear lacp counters	483
debug lacp	484
lacp port-priority	485
lacp system-priority	486
lacp timeout	487
show debugging lacp	489
show diagnostic channel-group	490
show etherchannel	491
show etherchannel detail	492
show etherchannel summary	493
show lacp sys-id	494
show lacp-counter	495
show port etherchannel	496

	show static-channel-group	498
	static-channel-group	499
	undebg lacp	501
Chapter 14:	Power over Ethernet Commands	502
	Introduction	502
	clear power-inline counters interface	504
	debug power-inline	505
	power-inline allow-legacy	507
	power-inline description	508
	power-inline enable	509
	power-inline max	510
	power-inline priority	512
	power-inline usage-threshold	514
	service power-inline	515
	show debugging power-inline	516
	show power-inline	517
	show power-inline counters	519
	show power-inline interface	521
	show power-inline interface detail	523
Chapter 15:	GVRP Commands	526
	Introduction	526
	clear gvrp statistics	527
	debug gvrp	528
	gvrp (interface)	530
	gvrp dynamic-vlan-creation	531
	gvrp enable (global)	532
	gvrp registration	533
	gvrp timer	534
	show debugging gvrp	535
	show gvrp configuration	536
	show gvrp machine	537
	show gvrp statistics	538
	show gvrp timer	539
Chapter 16:	IP Addressing and Protocol Commands	540
	Introduction	540
	arp-aging-timeout	542
	arp-mac-disparity	543
	arp (IP address MAC)	544
	arp log	545
	clear arp-cache	549
	debug ip packet interface	550
	ip address	552
	ip domain-list	554
	ip domain-lookup	555
	ip domain-name	556
	ip gratuitous-arp-link	557
	ip name-server	559
	ping	560
	show arp	561

	show debugging ip packet	563
	show hosts	565
	show ip domain-list	566
	show ip domain-name	567
	show ip interface	568
	show ip name-server	569
	show ip sockets	570
	show ip traffic	573
	tcpdump	579
	tracert	580
	undebg ip packet interface	581
Chapter 17:	IPv6 Commands	582
	Introduction	582
	clear ipv6 neighbors	583
	ipv6 address	584
	ipv6 address autoconfig	585
	ipv6 enable	587
	ipv6 nd raguard	589
	ipv6 neighbor	591
	ipv6 route	592
	ping ipv6	593
	show ipv6 interface brief	594
	show ipv6 neighbors	595
	show ipv6 route	596
	show ipv6 route summary	598
	tracert ipv6	599
Chapter 18:	Static Routing Commands for Management Purposes	600
	Introduction	600
	ip route	601
	show ip route	602
	show ip route database	604
	show ip route summary	605
Chapter 19:	Multicast Commands	606
	Introduction	606
	clear ip mroute	608
	clear ip mroute statistics	609
	clear ipv6 mroute	610
	clear ipv6 mroute statistics	611
	debug nsm mcast	612
	debug nsm mcast6	613
	ip mroute	614
	ip multicast forward-first-packet	616
	ip multicast route	617
	ip multicast route-limit	619
	ip multicast wrong-vif-suppression	620
	ip multicast-routing	621
	ipv6 multicast route	622
	ipv6 multicast route-limit	624
	ipv6 multicast-routing	625

	multicast	626
	show ip mroute	627
	show ip mvif	629
	show ip rpf	630
	show ipv6 mroute	631
	show ipv6 mif	633
Chapter 20:	IGMP Snooping Commands	634
	Introduction	634
	clear ip igmp	635
	clear ip igmp group	636
	clear ip igmp interface	637
	debug igmp	638
	ip igmp snooping	639
	ip igmp snooping fast-leave	640
	ip igmp snooping querier	641
	ip igmp snooping report-suppression	642
	ip igmp snooping tcn query solicit	643
	ip igmp static-group	645
	ip igmp version	647
	show debugging igmp	648
	show ip igmp groups	649
	show ip igmp interface	651
	show ip igmp snooping statistics	654
	undebug igmp	655
Chapter 21:	MLD Snooping Commands	656
	Introduction	656
	clear ipv6 mld	657
	clear ipv6 mld group	658
	clear ipv6 mld interface	659
	debug mld	660
	ipv6 mld access-group	661
	ipv6 mld limit	662
	ipv6 mld snooping	664
	ipv6 mld snooping fast-leave	666
	ipv6 mld snooping mrouter	667
	ipv6 mld snooping querier	669
	ipv6 mld snooping report-suppression	670
	ipv6 mld static-group	672
	show debugging mld	674
	show ipv6 mld groups	675
	show ipv6 mld interface	676
	show ipv6 mld snooping mrouter	677
	show ipv6 mld snooping statistics	678
Chapter 22:	IPv4 Hardware Access Control List (ACL) Commands	679
	Introduction	679
	access-group	681
	access-list (hardware IP numbered)	683
	access-list (hardware MAC numbered)	691
	access-list hardware (named)	693

	(access-list hardware ICMP filter)	695
	(access-list hardware IP protocol filter)	698
	(access-list hardware MAC filter)	704
	(access-list hardware TCP UDP filter)	707
	commit (IPv4)	710
	show access-list (IPv4 Hardware ACLs)	711
	show interface access-group	713
Chapter 23:	IPv4 Software Access Control List (ACL) Commands	714
	Introduction	714
	access-list extended (named)	716
	access-list (extended numbered)	724
	(access-list extended ICMP filter)	726
	(access-list extended IP filter)	728
	(access-list extended IP protocol filter)	731
	(access-list extended TCP UDP filter)	736
	access-list standard (named)	738
	access-list (standard numbered)	740
	(access-list standard named filter)	742
	(access-list standard numbered filter)	744
	clear ip prefix-list	746
	ip prefix-list	747
	maximum-access-list	749
	show access-list (IPv4 Software ACLs)	750
	show ip access-list	752
Chapter 24:	IPv6 Hardware Access Control List (ACL) Commands	753
	Introduction	753
	commit (IPv6)	755
	ipv6 access-list (named)	756
	(ipv6 access-list named ICMP filter)	758
	(ipv6 access-list named protocol filter)	761
	(ipv6 access-list named TCP UDP filter)	765
	ipv6 traffic-filter	768
	show ipv6 access-list (IPv6 Hardware ACLs)	769
Chapter 25:	IPv6 Software Access Control List (ACL) Commands	771
	Introduction	771
	ipv6 access-list standard (named)	773
	(ipv6 access-list standard filter)	775
	show ipv6 access-list (IPv6 Software ACLs)	777
Chapter 26:	QoS Commands	778
	Introduction	778
	class	780
	class-map	781
	default-action	782
	description (QoS policy-map)	783
	egress-rate-limit	784
	match access-group	785
	match cos	787
	match dscp	788

match eth-format protocol	789
match mac-type	792
match tcp-flags	793
match vlan	794
mls qos cos	795
mls qos cpu-queue rx-rate-limit	796
mls qos enable	797
mls qos map cos-queue to	798
mls qos map premark-dscp to	799
no police	800
police single-rate action	801
policy-map	802
priority-queue	803
remark new-cos	804
service-policy input	805
show class-map	806
show mls qos	807
show mls qos interface	808
show mls qos maps cos-queue	810
show policy-map	811
trust dscp	812
wrr-queue weight queues	813

Chapter 27: 802.1X Commands 815

Introduction	815
debug dot1x	816
dot1x control-direction	817
dot1x eap	818
dot1x eapol-version	819
dot1x initialize interface	820
dot1x initialize supplicant	821
dot1x keytransmit	822
dot1x max-auth-fail	823
dot1x max-reauth-req	825
dot1x port-control	826
dot1x timeout tx-period	828
show debugging dot1x	829
show dot1x	830
show dot1x diagnostics	833
show dot1x interface	835
show dot1x sessionstatistics	840
show dot1x statistics interface	841
show dot1x supplicant	842
show dot1x supplicant interface	844
undebg dot1x	847

Chapter 28: Authentication Commands 848

Introduction	848
auth auth-fail vlan	851
auth critical	853
auth dynamic-vlan-creation	854
auth guest-vlan	857

auth host-mode	859
auth log	861
auth max-supPLICant	863
auth reauthentication	864
auth roaming disconnected	865
auth roaming enable	867
auth supplicant-mac	869
auth timeout connect-timeout	871
auth timeout quiet-period	872
auth timeout reauth-period	873
auth timeout server-timeout	874
auth timeout supp-timeout	875
auth two-step enable	876
auth-mac enable	879
auth-mac method	881
auth-mac password	882
auth-mac reauth-relearning	883
auth-web enable	884
auth-web forward	885
auth-web max-auth-fail	887
auth-web method	888
auth-web-server blocking-mode	889
auth-web-server dhcp ipaddress	890
auth-web-server dhcp lease	891
auth-web-server dhcp-wpad-option	892
auth-web-server gateway (deleted)	893
auth-web-server host-name	894
auth-web-server http-redirect (deleted)	895
auth-web-server intercept-port	896
auth-web-server ipaddress	897
auth-web-server login-url	898
auth-web-server mode (deleted)	899
auth-web-server page logo	900
auth-web-server page sub-title	901
auth-web-server page success-message	902
auth-web-server page title	903
auth-web-server page welcome-message	904
auth-web-server ping-poll enable	905
auth-web-server ping-poll failcount	906
auth-web-server ping-poll interval	907
auth-web-server ping-poll reauth-timer-refresh	908
auth-web-server ping-poll timeout	909
auth-web-server port	910
auth-web-server redirect-delay-time	911
auth-web-server redirect-url	912
auth-web-server session-keep	913
auth-web-server ssl	914
auth-web-server sslport (deleted)	915
auth-web-server ssl intercept-port	916
copy proxy-autoconfig-file	917
copy web-auth-https-file	918
erase proxy-autoconfig-file	919
erase web-auth-https-file	920

show auth two-step supplicant brief	921
show auth-mac	922
show auth-mac diagnostics	923
show auth-mac interface	924
show auth-mac sessionstatistics	926
show auth-mac statistics interface	927
show auth-mac supplicant	928
show auth-mac supplicant interface	929
show auth-web	930
show auth-web diagnostics	932
show auth-web interface	934
show auth-web sessionstatistics	937
show auth-web statistics interface	938
show auth-web supplicant	939
show auth-web supplicant interface	940
show auth-web-server	941
show auth-web-server page	942
show proxy-autoconfig-file	943

Chapter 29: AAA Commands 944

Introduction	944
aaa accounting auth-mac default	946
aaa accounting auth-web default	948
aaa accounting commands	950
aaa accounting dot1x	952
aaa accounting login	954
aaa accounting update	957
aaa authentication auth-mac	959
aaa authentication auth-web	960
aaa authentication dot1x	961
aaa authentication enable default group tacacs+	962
aaa authentication enable default local	964
aaa authentication login	965
aaa group server	967
aaa local authentication attempts lockout-time	969
aaa local authentication attempts max-fail	970
accounting login	971
clear aaa local user lockout	972
debug aaa	973
login authentication	974
show aaa local user locked	975
show debugging aaa	976
undebug aaa	977

Chapter 30: RADIUS Commands 978

Introduction	978
deadtime (RADIUS server group)	979
debug radius	980
ip radius source-interface	981
radius-server deadtime	982
radius-server host	983
radius-server key	986

	radius-server retransmit	987
	radius-server timeout	989
	server (Server Group)	991
	show debugging radius	993
	show radius	994
	show radius statistics	996
	undebg radius	997
Chapter 31:	TACACS+ Commands	998
	Introduction	998
	show tacacs+	999
	tacacs-server host	1000
	tacacs-server key	1002
	tacacs-server timeout	1003
Chapter 32:	Secure Shell (SSH) Commands	1004
	Introduction	1004
	banner login (SSH)	1006
	clear ssh	1007
	crypto key destroy hostkey	1008
	crypto key destroy userkey	1009
	crypto key generate hostkey	1010
	crypto key generate userkey	1011
	crypto key pubkey-chain knownhosts	1012
	crypto key pubkey-chain userkey	1014
	debug ssh client	1016
	debug ssh server	1017
	service ssh	1018
	show banner login	1020
	show crypto key hostkey	1021
	show crypto key pubkey-chain knownhosts	1022
	show crypto key pubkey-chain userkey	1023
	show crypto key userkey	1024
	show running-config ssh	1025
	show ssh	1027
	show ssh client	1029
	show ssh server	1030
	show ssh server allow-users	1032
	show ssh server deny-users	1033
	ssh	1034
	ssh client	1036
	ssh server	1038
	ssh server allow-users	1040
	ssh server authentication	1042
	ssh server deny-users	1044
	ssh server resolve-host	1046
	ssh server scp	1047
	ssh server sftp	1048
	undebg ssh client	1049
	undebg ssh server	1050
Chapter 33:	DHCP Snooping Commands	1051

	Introduction	1051
	arp security	1053
	arp security violation	1054
	clear arp security statistics	1056
	clear ip dhcp snooping binding	1057
	clear ip dhcp snooping statistics	1058
	debug arp security	1059
	debug ip dhcp snooping	1060
	ip dhcp snooping	1061
	ip dhcp snooping agent-option	1062
	ip dhcp snooping agent-option allow-untrusted	1063
	ip dhcp snooping agent-option circuit-id vlantriplet	1064
	ip dhcp snooping agent-option remote-id	1065
	ip dhcp snooping binding	1066
	ip dhcp snooping database	1067
	ip dhcp snooping delete-by-client	1068
	ip dhcp snooping delete-by-linkdown	1069
	ip dhcp snooping max-bindings	1070
	ip dhcp snooping subscriber-id	1071
	ip dhcp snooping trust	1072
	ip dhcp snooping verify mac-address	1073
	ip dhcp snooping violation	1074
	ip source binding	1075
	service dhcp-snooping	1077
	show arp security	1079
	show arp security interface	1080
	show arp security statistics	1082
	show debugging arp security	1085
	show debugging ip dhcp snooping	1086
	show ip dhcp snooping	1087
	show ip dhcp snooping acl	1088
	show ip dhcp snooping agent-option	1091
	show ip dhcp snooping binding	1094
	show ip dhcp snooping interface	1096
	show ip dhcp snooping statistics	1098
	show ip source binding	1102
Chapter 34:	RRP Snooping Commands	1103
	Introduction	1103
	ip rrp snooping	1104
	show ip rrp snooping	1105
Chapter 35:	EPSR Commands	1106
	Introduction	1106
	debug epsr	1108
	epsr	1109
	epsr configuration	1110
	epsr datavlan	1111
	epsr enhancedrecovery enable	1112
	epsr mode master controlvlan primary port	1113
	epsr mode transit controlvlan	1114
	epsr priority	1115

epsr state	1116
epsr trap	1117
show debugging epsr	1118
show epsr	1119
show epsr common segments	1125
show epsr config-check	1126
show epsr <epsr-instance>	1128
show epsr <epsr-instance> counters	1129
show epsr counters	1130
show epsr summary	1131
undebg epsr	1132

Chapter 36:

AMF Commands 1133

Introduction	1133
atmf area	1136
atmf area password	1137
atmf backup	1139
atmf backup area-masters delete	1140
atmf backup area-masters enable	1141
atmf backup area-masters now	1142
atmf backup area-masters synchronize	1143
atmf backup bandwidth	1144
atmf backup delete	1145
atmf backup enable	1146
atmf backup now	1147
atmf backup server	1149
atmf backup stop	1151
atmf backup synchronize	1152
atmf cleanup	1153
atmf controller	1154
atmf distribute firmware	1155
atmf domain vlan	1157
atmf enable	1159
atmf group (membership)	1160
atmf log-verbose	1162
atmf management subnet	1163
atmf management vlan	1165
atmf master	1166
atmf network-name	1167
atmf provision	1168
atmf provision node clone	1169
atmf provision node configure boot config	1171
atmf provision node configure boot system	1173
atmf provision node create	1175
atmf provision node delete	1177
atmf provision node license-cert	1179
atmf provision node locate	1181
atmf reboot-rolling	1182
atmf recover	1186
atmf recover led-off	1188
atmf remote-login	1189
atmf restricted-login	1190
atmf select-area	1191

atmf virtual-link	1192
atmf working-set	1195
clear atmf links statistics	1197
debug atmf	1198
debug atmf packet	1200
erase factory-default	1203
show atmf	1204
show atmf area	1208
show atmf area summary	1211
show atmf area nodes	1212
show atmf area nodes-detail	1214
show atmf backup	1216
show atmf backup area	1219
show atmf detail	1221
show atmf group	1223
show atmf group members	1225
show atmf links	1227
show atmf links detail	1228
show atmf links statistics	1236
show atmf memory	1241
show atmf nodes	1243
show atmf provision nodes	1244
show atmf tech	1245
show atmf working-set	1248
show debugging atmf	1249
show debugging atmf packet	1250
show running-config atmf	1251
switchport atmf-arealink remote-area	1252
switchport atmf-crosslink	1253
switchport atmf-link	1255
type atmf node	1256
undebg atmf	1259

Chapter 37: NTP Commands 1260

Introduction	1260
ntp access-group	1261
ntp authenticate	1262
ntp authentication-key	1263
ntp broadcastdelay	1264
ntp master	1265
ntp peer	1266
ntp server	1268
ntp source	1270
ntp trusted-key	1272
show counter ntp	1273
show ntp associations	1275
show ntp status	1277

Chapter 38: Dynamic Host Configuration Protocol (DHCP) Commands 1278

Introduction	1278
ip address dhcp	1279
show counter dhcp-client	1281

	show dhcp lease	1282
Chapter 39:	DHCP for IPv6 (DHCPv6) Commands	1284
	Introduction	1284
	clear counter ipv6 dhcp-client	1285
	clear ipv6 dhcp client	1286
	ipv6 address dhcp	1287
	show counter ipv6 dhcp-client	1288
	show ipv6 dhcp	1290
	show ipv6 dhcp interface	1291
Chapter 40:	SNMP Commands	1292
	Introduction	1292
	debug snmp	1294
	show counter snmp-server	1295
	show debugging snmp	1300
	show running-config snmp	1301
	show snmp-server	1302
	show snmp-server community	1303
	show snmp-server group	1304
	show snmp-server user	1305
	show snmp-server view	1306
	snmp trap link-status	1307
	snmp trap link-status suppress	1309
	snmp-server	1311
	snmp-server community	1313
	snmp-server contact	1314
	snmp-server enable trap	1315
	snmp-server engineID local	1317
	snmp-server engineID local reset	1319
	snmp-server group	1320
	snmp-server host	1322
	snmp-server location	1324
	snmp-server source-interface	1325
	snmp-server startup-trap-delay	1326
	snmp-server user	1327
	snmp-server view	1330
	undebg snmp	1331
Chapter 41:	LLDP Commands	1332
	Introduction	1332
	clear lldp statistics	1334
	clear lldp table	1335
	debug lldp	1336
	lldp faststart-count	1338
	lldp holdtime-multiplier	1339
	lldp management-address	1340
	lldp med-notifications	1341
	lldp med-tlv-select	1342
	lldp non-strict-med-tlv-order-check	1344
	lldp notification-interval	1345
	lldp notifications	1346

	lldp port-number-type	1347
	lldp reinit	1348
	lldp run	1349
	lldp timer	1350
	lldp tlv-select	1351
	lldp transmit receive	1353
	lldp tx-delay	1354
	location civic-location configuration	1355
	location civic-location identifier	1360
	location civic-location-id	1361
	location coord-location configuration	1362
	location coord-location identifier	1364
	location coord-location-id	1365
	location elin-location	1366
	location elin-location-id	1367
	show debugging lldp	1368
	show lldp	1370
	show lldp interface	1372
	show lldp local-info	1374
	show lldp neighbors	1379
	show lldp neighbors detail	1381
	show lldp statistics	1385
	show lldp statistics interface	1387
	show location	1390
Chapter 42:	SMTP Commands	1392
	Introduction	1392
	debug mail	1393
	delete mail	1394
	mail	1395
	mail from	1396
	mail smtpserver	1397
	show counter mail	1398
	show mail	1399
	undebg mail	1400
Chapter 43:	RMON Commands	1401
	Introduction	1401
	rmon alarm	1402
	rmon collection history	1404
	rmon collection stats	1405
	rmon event	1406
	show rmon alarm	1407
	show rmon event	1408
	show rmon history	1410
	show rmon statistics	1412
Chapter 44:	Trigger Commands	1414
	Introduction	1414
	active (trigger)	1416
	day	1417
	debug trigger	1419

description (trigger)	1420
repeat	1421
script	1422
show debugging trigger	1424
show running-config trigger	1425
show trigger	1426
test	1431
time (trigger)	1432
trap	1434
trigger	1435
trigger activate	1436
type atmf node	1437
type cpu	1440
type interface	1441
type memory	1442
type periodic	1443
type ping-poll	1444
type reboot	1445
type time	1446
type usb	1447
undebg trigger	1448

Chapter 45: Ping-Polling Commands 1449

Introduction	1449
active (ping-polling)	1451
clear ping-poll	1452
critical-interval	1453
debug ping-poll	1454
description (ping-polling)	1455
fail-count	1456
ip (ping-polling)	1457
length (ping-poll data)	1458
normal-interval	1459
ping-poll	1460
sample-size	1461
show counter ping-poll	1463
show ping-poll	1466
source-ip	1471
timeout (ping polling)	1472
up-count	1473
undebg ping-poll	1474

List of Commands

(access-list extended ICMP filter)	726
(access-list extended IP filter).....	728
(access-list extended IP protocol filter).....	731
(access-list extended TCP UDP filter).....	736
(access-list hardware ICMP filter)	695
(access-list hardware IP protocol filter).....	698
(access-list hardware MAC filter).....	704
(access-list hardware TCP UDP filter).....	707
(access-list standard named filter)	742
(access-list standard numbered filter).....	744
(ipv6 access-list named ICMP filter)	758
(ipv6 access-list named protocol filter).....	761
(ipv6 access-list named TCP UDP filter)	765
(ipv6 access-list standard filter).....	775
aaa accounting auth-mac default.....	946
aaa accounting auth-web default	948
aaa accounting commands.....	950
aaa accounting dot1x.....	952
aaa accounting login.....	954
aaa accounting update.....	957
aaa authentication auth-mac.....	959
aaa authentication auth-web.....	960
aaa authentication dot1x	961
aaa authentication enable default group tacacs+	962
aaa authentication enable default local.....	964

aaa authentication login	965
aaa group server.....	967
aaa local authentication attempts lockout-time.....	969
aaa local authentication attempts max-fail	970
access-group	681
access-list (extended numbered).....	724
access-list (hardware IP numbered).....	683
access-list (hardware MAC numbered).....	691
access-list (standard numbered).....	740
access-list extended (named)	716
access-list hardware (named)	693
access-list standard (named)	738
accounting login	971
activate	281
active (ping-polling)	1451
active (trigger).....	1416
alarm facility.....	304
arp (IP address MAC).....	544
arp log	545
arp security violation	1054
arp security.....	1053
arp-aging-timeout.....	542
arp-mac-disparity.....	543
atmf area password.....	1137
atmf area.....	1136
atmf backup area-masters delete.....	1140
atmf backup area-masters enable	1141
atmf backup area-masters now.....	1142
atmf backup area-masters synchronize	1143
atmf backup bandwidth	1144
atmf backup delete	1145
atmf backup enable	1146
atmf backup now.....	1147
atmf backup server	1149
atmf backup stop.....	1151

atmf backup synchronize	1152
atmf backup.....	1139
atmf cleanup	1153
atmf controller	1154
atmf distribute firmware	1155
atmf domain vlan.....	1157
atmf enable	1159
atmf group (membership)	1160
atmf log-verbose	1162
atmf management subnet	1163
atmf management vlan	1165
atmf master	1166
atmf network-name	1167
atmf provision node clone	1169
atmf provision node configure boot config	1171
atmf provision node configure boot system	1173
atmf provision node create	1175
atmf provision node delete	1177
atmf provision node license-cert	1179
atmf provision node locate.....	1181
atmf provision.....	1168
atmf reboot-rolling	1182
atmf recover led-off.....	1188
atmf recover.....	1186
atmf remote-login	1189
atmf restricted-login.....	1190
atmf select-area	1191
atmf virtual-link	1192
atmf working-set	1195
auth auth-fail vlan	851
auth critical.....	853
auth dynamic-vlan-creation.....	854
auth guest-vlan.....	857
auth host-mode	859
auth log	861

auth max-supPLICant.....	863
auth reauthentication.....	864
auth roaming disconnected.....	865
auth roaming enable	867
auth supplicant-mac.....	869
auth timeout connect-timeout.....	871
auth timeout quiet-period	872
auth timeout reauth-period.....	873
auth timeout server-timeout.....	874
auth timeout supp-timeout.....	875
auth two-step enable.....	876
auth-mac enable	879
auth-mac method	881
auth-mac password.....	882
auth-mac reauth-relearning.....	883
auth-web enable	884
auth-web forward	885
auth-web max-auth-fail.....	887
auth-web method	888
auth-web-server blocking-mode	889
auth-web-server dhcp ipaddress.....	890
auth-web-server dhcp lease.....	891
auth-web-server dhcp-wpad-option	892
auth-web-server gateway (deleted)	893
auth-web-server host-name.....	894
auth-web-server http-redirect (deleted)	895
auth-web-server intercept-port	896
auth-web-server ipaddress.....	897
auth-web-server login-url.....	898
auth-web-server mode (deleted)	899
auth-web-server page logo	900
auth-web-server page sub-title.....	901
auth-web-server page success-message.....	902
auth-web-server page title.....	903
auth-web-server page welcome-message	904

auth-web-server ping-poll enable	905
auth-web-server ping-poll failcount	906
auth-web-server ping-poll interval	907
auth-web-server ping-poll reauth-timer-refresh	908
auth-web-server ping-poll timeout.....	909
auth-web-server port	910
auth-web-server redirect-delay-time	911
auth-web-server redirect-url	912
auth-web-server session-keep	913
auth-web-server ssl intercept-port	916
auth-web-server ssl	914
auth-web-server sslport (deleted)	915
autoboot enable.....	107
backpressure	311
banner exec	162
banner login (SSH).....	1006
banner login (system).....	164
banner motd	166
boot config-file backup	110
boot config-file	108
boot system backup	113
boot system	111
cd	114
channel-group	481
class.....	780
class-map	781
clear aaa local user lockout.....	972
clear arp security statistics	1056
clear arp-cache	549
clear atmf links statistics	1197
clear counter ipv6 dhcp-client.....	1285
clear exception log	229
clear gvrp statistics	527
clear ip dhcp snooping binding	1057
clear ip dhcp snooping statistics	1058

clear ip igmp group.....	636
clear ip igmp interface	637
clear ip igmp	635
clear ip mroute statistics	609
clear ip mroute	608
clear ip prefix-list	746
clear ipv6 dhcp client	1286
clear ipv6 mld group.....	658
clear ipv6 mld interface	659
clear ipv6 mld	657
clear ipv6 mroute statistics.....	611
clear ipv6 mroute.....	610
clear ipv6 neighbors	583
clear lacp counters.....	483
clear line console	65
clear line vty.....	66
clear lldp statistics	1334
clear lldp table.....	1335
clear log buffered.....	231
clear log permanent	232
clear log.....	230
clear loop-protection counters	313
clear mac address-table dynamic.....	315
clear mac address-table static	314
clear ping-poll.....	1452
clear port counter	317
clear power-inline counters interface.....	504
clear spanning-tree detected protocols (RSTP and MSTP)	404
clear spanning-tree statistics.....	403
clear ssh.....	1007
clear test interface	299
clock set.....	168
clock summer-time date	169
clock summer-time recurring	171
clock timezone	173

commit (IPv4)	710
commit (IPv6)	755
configure terminal	53
continuous-reboot-prevention	174
copy (filename)	119
copy current-software	115
copy debug	116
copy proxy-autoconfig-file	917
copy running-config	117
copy startup-config	118
copy web-auth-https-file	918
copy zmodem	121
create autoboot	122
critical-interval	1453
crypto key destroy hostkey	1008
crypto key destroy userkey	1009
crypto key generate hostkey	1010
crypto key generate userkey	1011
crypto key pubkey-chain knownhosts	1012
crypto key pubkey-chain userkey	1014
day	1417
deadtime (RADIUS server group)	979
debug aaa	973
debug arp security	1059
debug atmf packet	1200
debug atmf	1198
debug dot1x	816
debug epsr	1108
debug gvrp	528
debug igmp	638
debug ip dhcp snooping	1060
debug ip packet interface	550
debug lacp	484
debug lldp	1336
debug loopprot	318

debug mail	1393
debug mld	660
debug mstp (RSTP and STP)	405
debug nsm mcast	612
debug nsm mcast6	613
debug ping-poll	1454
debug platform packet	319
debug power-inline	505
debug radius	980
debug snmp	1294
debug ssh client	1016
debug ssh server	1017
debug trigger	1419
default log buffered	233
default log console	234
default log email	235
default log host	236
default log monitor	237
default log permanent	238
default-action	782
delete debug	124
delete mail	1394
delete	123
description (interface)	285
description (ping-polling)	1455
description (QoS policy-map)	783
description (trigger)	1420
dir	125
disable (Privileged Exec mode)	54
do	55
dot1x control-direction	817
dot1x eap	818
dot1x eapol-version	819
dot1x initialize interface	820
dot1x initialize supplicant	821

dot1x keytransmit	822
dot1x max-auth-fail	823
dot1x max-reauth-req	825
dot1x port-control	826
dot1x timeout tx-period	828
duplex	321
echo	282
ecofriendly led	176
edit (filename)	128
edit	127
egress-rate-limit	784
enable (Privileged Exec mode)	56
enable password	67
enable secret	70
end	58
epsr configuration	1110
epsr datavlan	1111
epsr enhancedrecovery enable	1112
epsr mode master controlvlan primary port	1113
epsr mode transit controlvlan	1114
epsr priority	1115
epsr state	1116
epsr trap	1117
epsr	1109
erase factory-default	1203
erase proxy-autoconfig-file	919
erase startup-config	130
erase web-auth-https-file	920
exec-timeout	73
exit	59
fail-count	1456
findme	177
flowcontrol (switch port)	322
flowcontrol hardware (asyn/console)	75
gvrp (interface)	530

gvrp dynamic-vlan-creation.....	531
gvrp enable (global)	532
gvrp registration.....	533
gvrp timer.....	534
help.....	60
hostname	178
instance priority (MSTP).....	409
instance vlan (MSTP).....	411
interface (to configure)	286
ip (ping-polling)	1457
ip address dhcp	1279
ip address	552
ip dhcp snooping agent-option allow-untrusted.....	1063
ip dhcp snooping agent-option circuit-id vlantriplet	1064
ip dhcp snooping agent-option remote-id.....	1065
ip dhcp snooping agent-option	1062
ip dhcp snooping binding	1066
ip dhcp snooping database	1067
ip dhcp snooping delete-by-client	1068
ip dhcp snooping delete-by-linkdown.....	1069
ip dhcp snooping max-bindings	1070
ip dhcp snooping subscriber-id	1071
ip dhcp snooping trust.....	1072
ip dhcp snooping verify mac-address.....	1073
ip dhcp snooping violation.....	1074
ip dhcp snooping.....	1061
ip domain-list.....	554
ip domain-lookup	555
ip domain-name.....	556
ip gratuitous-arp-link	557
ip igmp snooping fast-leave.....	640
ip igmp snooping querier.....	641
ip igmp snooping report-suppression	642
ip igmp snooping tcn query solicit	643
ip igmp snooping.....	639

ip igmp static-group	645
ip igmp version	647
ip mroute	614
ip multicast forward-first-packet	616
ip multicast route	617
ip multicast route-limit	619
ip multicast wrong-vif-suppression	620
ip multicast-routing	621
ip name-server	559
ip prefix-list	747
ip radius source-interface	981
ip route	601
ip rrp snooping	1104
ip source binding	1075
ipv6 access-list (named)	756
ipv6 access-list standard (named)	773
ipv6 address autoconfig	585
ipv6 address dhcp	1287
ipv6 address	584
ipv6 enable	587
ipv6 mld access-group	661
ipv6 mld limit	662
ipv6 mld snooping fast-leave	666
ipv6 mld snooping mrouter	667
ipv6 mld snooping querier	669
ipv6 mld snooping report-suppression	670
ipv6 mld snooping	664
ipv6 mld static-group	672
ipv6 multicast route	622
ipv6 multicast route-limit	624
ipv6 multicast-routing	625
ipv6 nd raguard	589
ipv6 neighbor	591
ipv6 route	592
ipv6 traffic-filter	768

lacp port-priority	485
lacp system-priority.....	486
lacp timeout.....	487
length (asyn)	77
length (ping-poll data).....	1458
line.....	78
linkflap action	324
lldp faststart-count	1338
lldp holdtime-multiplier	1339
lldp management-address	1340
lldp med-notifications	1341
lldp med-tlv-select.....	1342
lldp non-strict-med-tlv-order-check	1344
lldp notification-interval	1345
lldp notifications	1346
lldp port-number-type.....	1347
lldp reinit.....	1348
lldp run	1349
lldp timer.....	1350
lldp tlv-select.....	1351
lldp transmit receive	1353
lldp tx-delay.....	1354
location civic-location configuration	1355
location civic-location identifier	1360
location civic-location-id.....	1361
location coord-location configuration	1362
location coord-location identifier	1364
location coord-location-id	1365
location elin-location	1366
location elin-location-id.....	1367
log buffered (filter)	240
log buffered size.....	243
log buffered.....	239
log console (filter)	245
log console.....	244

log email (filter).....	249
log email time	252
log email	248
log host (filter).....	255
log host time	258
log host	254
log monitor (filter)	260
log permanent (filter)	264
log permanent size	267
log permanent	263
login authentication	974
logout.....	61
log-rate-limit nsm	268
loop-protection action.....	326
loop-protection action-delay-time	327
loop-protection timeout	328
loop-protection	325
mac address-table acquire	329
mac address-table ageing-time	330
mac address-table static	331
mail from.....	1396
mail smtpserver	1397
mail	1395
match access-group	785
match cos	787
match dscp.....	788
match eth-format protocol.....	789
match mac-type	792
match tcp-flags.....	793
match vlan	794
maximum-access-list	749
mirror interface.....	332
mkdir	131
mls qos cos	795
mls qos cpu-queue rx-rate-limit	796

mls qos enable	797
mls qos map cos-queue to	798
mls qos map premark-dscp to	799
move debug	133
move	132
mru jumbo	288
mtu	289
multicast	626
no debug all	180
no police	800
normal-interval	1459
ntp access-group	1261
ntp authenticate	1262
ntp authentication-key	1263
ntp broadcastdelay	1264
ntp master	1265
ntp peer	1266
ntp server	1268
ntp source	1270
ntp trusted-key	1272
ping ipv6	593
ping	560
ping-poll	1460
platform stop-unreg-mc-flooding	334
platform vlan-stacking-tpid	336
polarity	337
police single-rate action	801
policy-map	802
port-vlan-forwarding-priority	360
power-inline allow-legacy	507
power-inline description	508
power-inline enable	509
power-inline max	510
power-inline priority	512
power-inline usage-threshold	514

priority-queue	803
private-vlan association	364
private-vlan	363
privilege level	80
pwd	134
radius-server deadtime	982
radius-server host	983
radius-server key	986
radius-server retransmit	987
radius-server timeout	989
reboot	181
region (MSTP)	413
reload	182
remark new-cos	804
repeat	1421
revision (MSTP)	414
rmdir	135
rmon alarm	1402
rmon collection history	1404
rmon collection stats	1405
rmon event	1406
sample-size	1461
script	1422
security-password forced-change	82
security-password history	81
security-password lifetime	83
security-password minimum-categories	84
security-password minimum-length	85
security-password reject-expired-pwd	86
security-password warning	87
server (Server Group)	991
service advanced-vty	88
service dhcp-snooping	1077
service password-encryption	89
service power-inline	515

service ssh.....	1018
service telnet.....	90
service terminal-length (deleted).....	91
service test.....	300
service-policy input.....	805
show aaa local user locked.....	975
show access-list (IPv4 Hardware ACLs).....	711
show access-list (IPv4 Software ACLs).....	750
show alarm settings.....	307
show arp security interface.....	1080
show arp security statistics.....	1082
show arp security.....	1079
show arp.....	561
show atmf area nodes.....	1212
show atmf area nodes-detail.....	1214
show atmf area summary.....	1211
show atmf area.....	1208
show atmf backup area.....	1219
show atmf backup.....	1216
show atmf detail.....	1221
show atmf group members.....	1225
show atmf group.....	1223
show atmf links detail.....	1228
show atmf links statistics.....	1236
show atmf links.....	1227
show atmf memory.....	1241
show atmf nodes.....	1243
show atmf provision nodes.....	1244
show atmf tech.....	1245
show atmf working-set.....	1248
show atmf.....	1204
show auth two-step supplicant brief.....	921
show auth-mac diagnostics.....	923
show auth-mac interface.....	924
show auth-mac sessionstatistics.....	926

show auth-mac statistics interface.....	927
show auth-mac supplicant interface.....	929
show auth-mac supplicant.....	928
show auth-mac.....	922
show auth-web diagnostics.....	932
show auth-web interface	934
show auth-web sessionstatistics	937
show auth-web statistics interface	938
show auth-web supplicant interface.....	940
show auth-web supplicant.....	939
show auth-web.....	930
show auth-web-server page	942
show auth-web-server.....	941
show autoboot	136
show banner login.....	1020
show boot.....	137
show class-map	806
show clock	183
show continuous-reboot-prevention.....	185
show counter dhcp-client.....	1281
show counter ipv6 dhcp-client.....	1288
show counter log.....	270
show counter mail.....	1398
show counter ntp.....	1273
show counter ping-poll.....	1463
show counter snmp-server.....	1295
show cpu history	189
show cpu.....	186
show crypto key hostkey.....	1021
show crypto key pubkey-chain knownhosts	1022
show crypto key pubkey-chain userkey.....	1023
show crypto key userkey.....	1024
show debugging aaa	976
show debugging arp security	1085
show debugging atmf packet	1250

show debugging atmf	1249
show debugging dot1x	829
show debugging epsr	1118
show debugging gvrp	535
show debugging igmp	648
show debugging ip dhcp snooping	1086
show debugging ip packet	563
show debugging lacp	489
show debugging lldp	1368
show debugging loopprot	338
show debugging mld	674
show debugging mstp	415
show debugging platform packet	339
show debugging power-inline	516
show debugging radius	993
show debugging snmp	1300
show debugging trigger	1424
show debugging	192
show dhcp lease	1282
show diagnostic channel-group	490
show dot1x diagnostics	833
show dot1x interface	835
show dot1x sessionstatistics	840
show dot1x statistics interface	841
show dot1x supplicant interface	844
show dot1x supplicant	842
show dot1x	830
show ecofriendly	193
show epsr <epsr-instance> counters	1129
show epsr <epsr-instance>	1128
show epsr common segments	1125
show epsr config-check	1126
show epsr counters	1130
show epsr summary	1131
show epsr	1119

show etherchannel detail	492
show etherchannel summary	493
show etherchannel	491
show exception log	271
show facility-alarm status	308
show file systems	140
show file	139
show flowcontrol interface	340
show gvrp configuration	536
show gvrp machine	537
show gvrp statistics	538
show gvrp timer	539
show history	62
show hosts	565
show interface access-group	713
show interface brief	294
show interface err-disabled	341
show interface memory	194
show interface status	295
show interface switchport	342
show interface	291
show ip access-list	752
show ip dhcp snooping acl	1088
show ip dhcp snooping agent-option	1091
show ip dhcp snooping binding	1094
show ip dhcp snooping interface	1096
show ip dhcp snooping statistics	1098
show ip dhcp snooping	1087
show ip domain-list	566
show ip domain-name	567
show ip igmp groups	649
show ip igmp interface	651
show ip igmp snooping statistics	654
show ip interface	568
show ip mroute	627

show ip mvif.....	629
show ip name-server.....	569
show ip route database.....	604
show ip route summary.....	605
show ip route.....	602
show ip rpf.....	630
show ip rrp snooping.....	1105
show ip sockets.....	570
show ip source binding.....	1102
show ip traffic.....	573
show ipv6 access-list (IPv6 Hardware ACLs).....	769
show ipv6 access-list (IPv6 Software ACLs).....	777
show ipv6 dhcp interface.....	1291
show ipv6 dhcp.....	1290
show ipv6 interface brief.....	594
show ipv6 mif.....	633
show ipv6 mld groups.....	675
show ipv6 mld interface.....	676
show ipv6 mld snooping mrouter.....	677
show ipv6 mld snooping statistics.....	678
show ipv6 mroute.....	631
show ipv6 neighbors.....	595
show ipv6 route summary.....	598
show ipv6 route.....	596
show lacp sys-id.....	494
show lacp-counter.....	495
show lldp interface.....	1372
show lldp local-info.....	1374
show lldp neighbors detail.....	1381
show lldp neighbors.....	1379
show lldp statistics interface.....	1387
show lldp statistics.....	1385
show lldp.....	1370
show location.....	1390
show log config.....	275

show log permanent.....	278
show log	272
show loop-protection.....	343
show mac address-table	344
show mail	1399
show memory allocations.....	198
show memory history.....	200
show memory pools	201
show memory shared.....	202
show memory	196
show mirror interface.....	347
show mirror	346
show mls qos interface.....	808
show mls qos maps cos-queue.....	810
show mls qos.....	807
show ntp associations	1275
show ntp status	1277
show ping-poll	1466
show platform classifier statistics utilization brief	349
show platform port	350
show platform.....	348
show policy-map	811
show port etherchannel	496
show port-vlan-forwarding-priority	365
show power-inline counters	519
show power-inline interface detail	523
show power-inline interface	521
show power-inline.....	517
show privilege.....	92
show process.....	203
show proxy-autoconfig-file	943
show radius statistics	996
show radius	994
show reboot history	205
show rmon alarm.....	1407

show rmon event.....	1408
show rmon history.....	1410
show rmon statistics.....	1412
show router-id.....	206
show running-config access-list.....	144
show running-config atmf.....	1251
show running-config dhcp.....	145
show running-config full.....	146
show running-config interface.....	147
show running-config ipv6 access-list.....	149
show running-config key chain.....	150
show running-config lldp.....	151
show running-config log.....	279
show running-config power-inline.....	152
show running-config router-id.....	153
show running-config security-password.....	154
show running-config snmp.....	1301
show running-config ssh.....	1025
show running-config trigger.....	1425
show running-config.....	142
show security-password configuration.....	93
show security-password user.....	94
show snmp-server community.....	1303
show snmp-server group.....	1304
show snmp-server user.....	1305
show snmp-server view.....	1306
show snmp-server.....	1302
show spanning-tree brief.....	419
show spanning-tree mst config.....	421
show spanning-tree mst detail interface.....	424
show spanning-tree mst detail interface.....	429
show spanning-tree mst detail.....	422
show spanning-tree mst instance interface.....	427
show spanning-tree mst instance.....	426
show spanning-tree mst interface.....	428

show spanning-tree mst	420
show spanning-tree statistics instance interface	435
show spanning-tree statistics instance	433
show spanning-tree statistics interface	437
show spanning-tree statistics	431
show spanning-tree vlan range-index	440
show spanning-tree	416
show ssh client	1029
show ssh server allow-users	1032
show ssh server deny-users	1033
show ssh server	1030
show ssh	1027
show startup-config	155
show static-channel-group	498
show system environment	208
show system interrupts	209
show system mac	210
show system pluggable detail	213
show system pluggable diagnostics	217
show system pluggable	211
show system serialnumber	219
show system	207
show tacacs+	999
show tech-support	220
show telnet	95
show trigger	1426
show users	96
show version	156
show vlan classifier group interface	368
show vlan classifier group	367
show vlan classifier interface group	369
show vlan classifier rule	370
show vlan private-vlan	371
show vlan	366
shutdown	297

snmp trap link-status suppress	1309
snmp trap link-status	1307
snmp-server community	1313
snmp-server contact	1314
snmp-server enable trap	1315
snmp-server engineID local reset	1319
snmp-server engineID local	1317
snmp-server group	1320
snmp-server host	1322
snmp-server location	1324
snmp-server source-interface	1325
snmp-server startup-trap-delay	1326
snmp-server user	1327
snmp-server view	1330
snmp-server	1311
source-ip	1471
spanning-tree autoedge (RSTP and MSTP)	441
spanning-tree bpdu	442
spanning-tree cisco-interoperability (MSTP)	444
spanning-tree edgeport (RSTP and MSTP)	445
spanning-tree enable	446
spanning-tree errdisable-timeout enable	448
spanning-tree errdisable-timeout interval	449
spanning-tree force-version	450
spanning-tree forward-time	451
spanning-tree guard root	452
spanning-tree hello-time	453
spanning-tree link-type	454
spanning-tree max-age	455
spanning-tree max-hops (MSTP)	456
spanning-tree mode	457
spanning-tree mst configuration	458
spanning-tree mst instance path-cost	460
spanning-tree mst instance priority	462
spanning-tree mst instance restricted-role	463

spanning-tree mst instance restricted-tcn	464
spanning-tree mst instance	459
spanning-tree path-cost	466
spanning-tree portfast (STP)	467
spanning-tree portfast bpdu-filter	469
spanning-tree portfast bpdu-guard	471
spanning-tree priority (bridge priority)	473
spanning-tree priority (port priority)	474
spanning-tree restricted-role	475
spanning-tree restricted-tcn	476
spanning-tree transmit-holdcount	477
speed (asyn)	222
speed	354
ssh client	1036
ssh server allow-users	1040
ssh server authentication	1042
ssh server deny-users	1044
ssh server resolve-host	1046
ssh server scp	1047
ssh server sftp	1048
ssh server	1038
ssh	1034
static-channel-group	499
switchport access vlan	372
switchport atmf-arealink remote-area	1252
switchport atmf-crosslink	1253
switchport atmf-link	1255
switchport enable vlan	373
switchport mode access	374
switchport mode private-vlan trunk promiscuous	376
switchport mode private-vlan trunk secondary	378
switchport mode private-vlan	375
switchport mode trunk	380
switchport private-vlan host-association	381
switchport private-vlan mapping	382

switchport trunk allowed vlan	383
switchport trunk native vlan	386
switchport vlan-stacking (double tagging)	388
switchport voice dscp	389
switchport voice vlan priority	392
switchport voice vlan	390
system territory (deprecated)	224
tacacs-server host	1000
tacacs-server key	1002
tacacs-server timeout	1003
tcpdump	579
telnet server	98
telnet	97
terminal length	99
terminal monitor	225
terminal resize	100
test interface	301
test	1431
time (trigger)	1432
timeout (ping polling)	1472
traceroute ipv6	599
traceroute	580
trap	1434
trigger activate	1436
trigger	1435
trust dscp	812
type atmf node	1256
type atmf node	1437
type cpu	1440
type interface	1441
type memory	1442
type periodic	1443
type ping-poll	1444
type reboot	1445
type time	1446

type usb.....	1447
undebug aaa	977
undebug all	226
undebug atmf.....	1259
undebug dot1x.....	847
undebug epsr	1132
undebug igmp	655
undebug ip packet interface	581
undebug lacp	501
undebug loopprot.....	356
undebug mail	1400
undebug mstp	478
undebug ping-poll	1474
undebug platform packet.....	357
undebug radius	997
undebug snmp.....	1331
undebug ssh client	1049
undebug ssh server.....	1050
undebug trigger.....	1448
up-count	1473
username	101
vlan classifier activate.....	394
vlan classifier group	395
vlan classifier rule ipv4.....	396
vlan classifier rule proto.....	397
vlan database	400
vlan	393
wait	283
write file.....	157
write memory	158
write terminal	159
wrr-queue weight queues.....	813

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 53
 - “[disable \(Privileged Exec mode\)](#)” on page 54
 - “[do](#)” on page 55
 - “[enable \(Privileged Exec mode\)](#)” on page 56
 - “[end](#)” on page 58
 - “[exit](#)” on page 59
 - “[help](#)” on page 60
 - “[logout](#)” on page 61
 - “[show history](#)” on page 62

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
<command>	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](#) 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 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](#) commands from the Global Configuration mode. The [service password-encryption](#) command encrypts passwords configured by the [enable password](#) and the [enable secret](#) 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](#) 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](#)

[exit](#)

[service password-encryption](#)

[username](#)

end

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

Syntax end

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

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

```
awplus# configure terminal
awplus(config)# interface vlan2
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 Global Configuration and Interface Configuration modes.

Example The following example shows the use of `exit` command to exit Interface mode, and return to Configure mode.

```
awplus# configure terminal
awplus(config)# interface vlan2
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 “Controlling “show” Command Output” in 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

User Access Commands

Introduction

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

- Command List**
- “clear line console” on page 65
 - “clear line vty” on page 66
 - “enable password” on page 67
 - “enable secret” on page 70
 - “exec-timeout” on page 73
 - “flowcontrol hardware (asyn/console)” on page 75
 - “length (asyn)” on page 77
 - “line” on page 78
 - “privilege level” on page 80
 - “security-password history” on page 81
 - “security-password forced-change” on page 82
 - “security-password lifetime” on page 83
 - “security-password minimum-categories” on page 84
 - “security-password minimum-length” on page 85
 - “security-password reject-expired-pwd” on page 86
 - “security-password warning” on page 87
 - “service advanced-vty” on page 88
 - “service password-encryption” on page 89
 - “service telnet” on page 90
 - “service terminal-length (deleted)” on page 91

- [“show privilege”](#) on page 92
- [“show security-password configuration”](#) on page 93
- [“show security-password user”](#) on page 94
- [“show telnet”](#) on page 95
- [“show users”](#) on page 96
- [“telnet”](#) on page 97
- [“telnet server”](#) on page 98
- [“terminal length”](#) on page 99
- [“terminal resize”](#) on page 100
- [“username”](#) on page 101

clear line console

Overview This command resets a console line. If a terminal session exists on the line then the terminal session is terminated. If console line settings have changed then the new settings are applied.

Syntax `clear line console 0`

Mode Privileged Exec

Example To reset the console line (asyn), use the command:

```
awplus# clear line console 0
```

```
awplus# % The new settings for console line 0 have been applied
```

Related Commands

- [clear line vty](#)
- [flowcontrol hardware \(asyn/console\)](#)
- [line](#)
- [show users](#)

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 To set a local password to control access to various privilege levels, use the [enable password](#) Global Configuration command. Use the [enable password](#) command to modify or create a password to be used, and use the [no enable password](#) command to remove the password.

Note that the [enable secret](#) command is an alias for the [enable password](#) command, and the [no enable secret](#) command is an alias for the [no enable password](#) command. Issuing a [no enable password](#) command removes a password configured with the [enable secret](#) command. The [enable password](#) command is shown in the running and startup configurations. Note that if the [enable secret](#) command is entered then [enable password](#) is shown in the configuration.

Syntax `enable password [<plain>|8 <hidden>|level <1-15> 8 <hidden>]`
`no enable password [level <1-15>]`

Parameter	Description
<plain>	Specifies the unencrypted password.
8	Specifies a hidden password will follow.
<hidden>	Specifies the hidden encrypted password. Use an encrypted password for better security where a password crosses the network or is stored on a TFTP server.
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 The privilege level for enable password is level 15 by default. Previously the default was level 1.

Mode Global Configuration

Usage This command enables the Network Administrator to set a password for entering the Privileged Exec mode when using the [enable \(Privileged Exec mode\)](#) command. There are three methods to enable a password. In the examples below, for each method, note that the configuration is different and the configuration file output is different, but the password string to be used to enter the Privileged Exec mode with the **enable** command is the same (**mypasswd**).

A user can now have an intermediate CLI security level set with this command for privilege level 7 to 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.

Note that the [enable password](#) command is an alias for the [enable secret](#) command and one password per privilege level is allowed using these commands. Do not assign one password to a privilege level with [enable password](#) and another password to a privilege level with [enable secret](#). Use [enable password](#) or [enable secret](#) commands. Do not use both on the same level.

Using plain passwords

The plain password is a clear text string that appears in the configuration file as configured.

```
awplus# configure terminal
awplus(config)# enable password mypasswd
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password mypasswd
!
interface lo
```

Using encrypted passwords

You can configure an encrypted password using the [service password-encryption](#) command. First, use the [enable password](#) command to specify the string that you want to use as a password (**mypasswd**). Then, use the [service password-encryption](#) command to encrypt the specified string (**mypasswd**). The advantage of using an encrypted password is that the configuration file does not show **mypasswd**, it will only show the encrypted string **fU7zHzuutY2SA**.

```
awplus# configure terminal
awplus(config)# enable password mypasswd
awplus(config)# service password-encryption
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password 8 fU7zHzuutY2SA
service password-encryption
!
interface lo
```

Using hidden passwords

You can configure an encrypted password using the **HIDDEN** parameter (**8**) with the [enable password](#) command. Use this method if you already know the encrypted string corresponding to the plain text string that you want to use as a password. It is not required to use the [service password-encryption](#) command for

this method. The output in the configuration file will show only the encrypted string, and not the text string.

```
awplus# configure terminal
awplus(config)# enable password 8 fU7zHzuutY2SA
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password 8 fU7zHzuutY2SA
!
interface lo
```

**Related
Commands**

[enable \(Privileged Exec mode\)](#)
[enable secret](#)
[service password-encryption](#)
[privilege level](#)
[show privilege](#)
[username](#)
[show running-config](#)

enable secret

Overview To set a local password to control access to various privilege levels, use the [enable secret](#) Global Configuration command. Use the [enable secret](#) command to modify or create a password to be used, and use the [no enable secret](#) command to remove the password.

Note that the [enable secret](#) command is an alias for the [enable password](#) command, and the [no enable secret](#) command is an alias for the [no enable password](#) command. Issuing a [no enable password](#) command removes a password configured with the [enable secret](#) command. The [enable password](#) command is shown in the running and startup configurations. Note that if the [enable secret](#) command is entered then [enable password](#) is shown in the configuration

Syntax `enable secret [<plain>|8 <hidden>|level <0-15> 8 <hidden>]`
`no enable secret [level <1-15>]`

Parameter	Description
<plain>	Specifies the unencrypted password.
8	Specifies a hidden password will follow.
<hidden>	Specifies the hidden encrypted password. Use an encrypted password for better security where a password crosses the network or is stored on a TFTP server.
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 The privilege level for enable secret is level 15 by default.

Mode Global Configuration

Usage This command enables the Network Administrator to set a password for entering the Privileged Exec mode when using the [enable \(Privileged Exec mode\)](#) command. There are three methods to enable a password. In the examples below, for each method, note that the configuration is different and the configuration file output is different, but the password string to be used to enter the Privileged Exec mode with the **enable** command is the same (**mypasswd**).

A user can have an intermediate CLI security level set with this command for privilege level 7 to 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.

Note that the [enable secret](#) command is an alias for the [enable password](#) command and one password per privilege level is allowed using these commands.

Do not assign one password to a privilege level with [enable password](#) and another password to a privilege level with [enable secret](#). Use [enable password](#) or [enable secret](#) commands. Do not use both on the same level.

Using plain passwords

The plain password is a clear text string that appears in the configuration file as configured.

```
awplus# configure terminal
awplus(config)# enable secret mypasswd
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password mypasswd
!
interface lo
```

Using encrypted passwords

Configure an encrypted password using the [service password-encryption](#) command. First, use the [enable password](#) command to specify the string that you want to use as a password (**mypasswd**). Then, use the [service password-encryption](#) command to encrypt the specified string (**mypasswd**). The advantage of using an encrypted password is that the configuration file does not show **mypasswd**, it will only show the encrypted string **fU7zHzuutY2SA**.

```
awplus# configure terminal
awplus(config)# enable secret mypasswd
awplus(config)# service password-encryption
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password 8 fU7zHzuutY2SA
service password-encryption
!
interface lo
```

Using hidden passwords

Configure an encrypted password using the **HIDDEN** parameter (**8**) with the **enable password** command. Use this method if you already know the encrypted string corresponding to the plain text string that you want to use as a password. It is not required to use the [service password-encryption](#) command for this method. The output in the configuration file will show only the encrypted string, and not the text string:

```
awplus# configure terminal
awplus(config)# enable secret 8 fU7zHzuutY2SA
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password 8 fU7zHzuutY2SA
!
interface lo
```

**Related
Commands**

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

[enable secret](#)

[service password-encryption](#)

[privilege level](#)

[show privilege](#)

[username](#)

[show running-config](#)

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 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
```

To reset the console connection to the default timeout of 10 minutes 0 seconds if there is no response from the user, use the following commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# no exec-timeout
```

Validation Commands `show running-config`

**Related
Commands** [line](#)
 [service telnet](#)

flowcontrol hardware (asyn/console)

Overview Use this command to enable RTS/CTS (Ready To Send/Clear To Send) hardware flow control on a terminal console line (asyn port) between the DTE (Data Terminal Equipment) and the DCE (Data Communications Equipment).

Syntax flowcontrol hardware
no flowcontrol hardware

Mode Line Configuration

Default Hardware flow control is disabled by default.

Usage Hardware flow control makes use of the RTS and CTS control signals between the DTE and DCE where the rate of transmitted data is faster than the rate of received data. Flow control is a technique for ensuring that a transmitting entity does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed.

Hardware flow control can be configured on terminal console lines (e.g. asyn0). For Reverse Telnet connections, hardware flow control must be configured to match on both the Access Server and the Remote Device. For terminal console sessions, hardware flow control must be configured to match on both the DTE and the DCE. Settings are saved in the running configuration. Changes are applied after reboot, clear line console, or after closing the session.

Use **show running-config** and **show startup-config** commands to view hardware flow control settings that take effect after reboot for a terminal console line. See the **show running-config** command output:

```
awplus#show running-config
!
line con 1
  speed 9600
  mode out 2001
  flowcontrol hardware
!
```

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 enable hardware flow control on terminal console line asyn0, use the commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# flowcontrol hardware
```

To disable hardware flow control on terminal console line asyn0, use the commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# no flowcontrol hardware
```

**Related
Commands**

- [clear line console](#)
- [show running-config](#)
- [speed \(asyn\)](#)

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 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 the console to 10 rows, use the command:

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

To reset the terminal session length on the console to the default (22 rows), use the command:

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

To display output to the console continuously, use the command:

```
awplus# configure terminal
awplus(config)# line console 0
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.
console	The console terminal line(s) for local access.
vtty	Virtual terminal for remote console access.

Mode Global Configuration

Usage In Line Configuration mode, you can configure console and virtual terminal settings, including setting [speed \(asyn\)](#), [length \(asyn\)](#), [privilege level](#), and authentication ([login authentication](#)) or accounting ([accounting login](#)) method lists.

To change the console (asyn) port speed, use this **line** command to enter Line Configuration mode before using the [speed \(asyn\)](#) command. Set the console speed (Baud rate) to match the transmission rate of the device connected to the console (asyn) port on your device.

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)#
```

To enter Line Configuration mode to configure the console (asyn 0) port terminal line, use the commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)#
```

**Related
Commands**

- accounting login
- clear line console
- clear line vty
- flowcontrol hardware (asyn/console)
- length (asyn)
- login authentication
- privilege level
- speed (asyn)

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 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 the console connection to have the maximum privilege level, use the following commands:

```
awplus# configure terminal
awplus(config)# line console 0
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 security-password history** command disables the security password history functionality.

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
```

Validation Commands show running-config security-password
show security-password configuration

Related Commands security-password forced-change
security-password lifetime
security-password minimum-categories
security-password minimum-length
security-password reject-expired-pwd
security-password warning

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 security-password forced-change** command disables the forced-change 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
```

Validation Commands [show running-config security-password](#)
[show security-password configuration](#)

Related Commands [security-password history](#)
[security-password lifetime](#)
[security-password minimum-categories](#)
[security-password minimum-length](#)
[security-password reject-expired-pwd](#)
[security-password warning](#)

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 security-password lifetime** command disables the password lifetime feature.

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

Parameter	Description
<0-1000>	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
```

Validation Commands show running-config security-password
show security-password configuration

Related Commands security-password history
security-password forced-change
security-password minimum-categories
security-password minimum-length
security-password reject-expired-pwd
security-password warning
show security-password user

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
```

Validation Commands [show running-config security-password](#)
[show security-password configuration](#)

Related Commands [security-password history](#)
[security-password forced-change](#)
[security-password lifetime](#)
[security-password minimum-length](#)
[security-password reject-expired-pwd](#)
[security-password warning](#)
[username](#)

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
<1 - 23>	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
```

Validation Commands show running-config security-password
show security-password configuration

Related Commands security-password history
security-password forced-change
security-password lifetime
security-password minimum-categories
security-password reject-expired-pwd
security-password warning
username

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 security-password reject-expired-pwd** command disables the reject-expired-pwd 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
```

Validation Commands [show running-config security-password](#)
[show security-password configuration](#)

Related Commands [security-password history](#)
[security-password forced-change](#)
[security-password lifetime](#)
[security-password minimum-categories](#)
[security-password minimum-length](#)
[security-password warning](#)
[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 security-password warning** 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
```

Validation Commands [show running-config security-password](#)
[show security-password configuration](#)

Related Commands [security-password history](#)
[security-password forced-change](#)
[security-password lifetime](#)
[security-password minimum-categories](#)
[security-password minimum-length](#)
[security-password reject-expired-pwd](#)

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](#)

service terminal-length (deleted)

Overview This command has been deleted.

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 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 2-1: 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 2-2: 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 [show running-config security-password](#)
[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 2-3: 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 [show running-config security-password](#)
[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 2-4: 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 2-5: 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 2-1: 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.

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
```

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
<length>	<0-512> 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 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 <0-15> [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><0-15></td><td> A privilege level: either 0 (no access), 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>	<0-15>	A privilege level: either 0 (no access), 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.		
<0-15>	A privilege level: either 0 (no access), 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> 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. Note that the user enters 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 23 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	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. Note that the user enters the plain-text version of the password when logging in.	<password>	The user's password. The password can be up to 23 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	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. Note that the user enters the plain-text version of the password when logging in.				
<password>	The user's password. The password can be up to 23 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 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.

A privilege level of 0 can be set for port authentication purposes from a RADIUS server.

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, for 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](#)

3

File Management Commands

Introduction

This chapter provides an alphabetical reference of AlliedWare Plus™ OS file 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 to or from a USB storage device	<code>usb: [/] [<directory> /] <filename></code>	To specify a file in the top-level directory of the USB stick: <code>usb: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: all printable ASCII characters not included in the previous three categories. Including the following characters:
 - -
 - /
 - .
 - _
 - @
 - "
 - '
 - *
 - :
 - ~
 - ?

Do not use spaces or parentheses within filenames. Use hyphens or underscores instead.

Syntax for directory listings

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

In commands where you need to specify the local filesystem'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:/`

Similarly, you can specify the USB storage device base directory with **usb** or **usb:** or **usb:/**

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

- ["autoboot enable"](#) on page 107
- ["boot config-file"](#) on page 108
- ["boot config-file backup"](#) on page 110
- ["boot system"](#) on page 111

- ["boot system backup"](#) on page 113
- ["cd"](#) on page 114
- ["copy current-software"](#) on page 115
- ["copy debug"](#) on page 116
- ["copy running-config"](#) on page 117
- ["copy startup-config"](#) on page 118
- ["copy \(filename\)"](#) on page 119
- ["copy zmodem"](#) on page 121
- ["create autoboot"](#) on page 122
- ["delete"](#) on page 123
- ["delete debug"](#) on page 124
- ["dir"](#) on page 125
- ["edit"](#) on page 127
- ["edit \(filename\)"](#) on page 128
- ["erase startup-config"](#) on page 130
- ["mkdir"](#) on page 131
- ["move"](#) on page 132
- ["move debug"](#) on page 133
- ["pwd"](#) on page 134
- ["rmdir"](#) on page 135
- ["show autoboot"](#) on page 136
- ["show boot"](#) on page 137
- ["show file"](#) on page 139
- ["show file systems"](#) on page 140
- ["show running-config"](#) on page 142
- ["show running-config access-list"](#) on page 144
- ["show running-config dhcp"](#) on page 145
- ["show running-config full"](#) on page 146
- ["show running-config interface"](#) on page 147
- ["show running-config ipv6 access-list"](#) on page 149
- ["show running-config key chain"](#) on page 150
- ["show running-config lldp"](#) on page 151
- ["show running-config power-inline"](#) on page 152
- ["show running-config router-id"](#) on page 153
- ["show running-config security-password"](#) on page 154

- [“show startup-config”](#) on page 155
- [“show version”](#) on page 156
- [“write file”](#) on page 157
- [“write memory”](#) on page 158
- [“write terminal”](#) on page 159

autoboot enable

This command enables the device to restore a release file and/or a configuration file from external media, such as a USB storage device.

When the Autoboot feature is enabled, the device looks for a special file called `autoboot . txt` on the external media. If this file exists, the device will check the key and values in the file and recover the device with a new release file and/or configuration file from the external media. An example of a valid `autoboot . txt` file is shown in the following figure.

Figure 3-1: Example `autoboot.txt` file

```
[AlliedWare Plus]
Copy_from_external_media_enabled=yes
Boot_Release=IE200-5.4.5I-01.rel
Boot_Config=network1.cfg
```

NOTE:

Syntax `autoboot enable`
 `no autoboot enable`

Default The Autoboot feature operates the first time the device is powered up in the field, after which the feature is disabled by default.

Mode Global Configuration

Example To enable the Autoboot feature, use the command:

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

To disable the Autoboot feature, use the command:

```
awplus# configure terminal
awplus(config)# no autoboot enable
```

**Related
Commands** `create autoboot`
 `show autoboot`
 `show boot`

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
<filepath-filename>	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 You can only specify that the configuration file is on a USB storage device if there is a backup configuration file already specified in Flash. If you attempt to set the configuration file on a USB storage device and a backup configuration file is not specified in Flash, the following error message is displayed:

```
% Backup configuration files must be stored in the flash filesystem
```

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` stored on the device's Flash filesystem the next time the device boots up, use the commands:

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

To remove the configuration file `branch.cfg` stored on the device's Flash filesystem the next time the device boots up, use the commands:

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

To run the configuration file `branch.cfg` stored on the switch's USB storage device filesystem the next time the device boots up, use the commands:

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

To remove the configuration file `branch.cfg` stored on the switch's USB storage device filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no boot config-file usb:/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
<filepath-filename>	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.
backup	The specified file is a backup configuration file.

Mode Global Configuration

Usage 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 remove the release file as the boot file.

Syntax boot system <filepath-filename>
no boot system

Parameter	Description
<filepath-filename>	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 You can only specify that the release file is on a USB storage device if there is a backup release file already specified in Flash. If you attempt to set the release file on a USB storage device and a backup release file is not specified in Flash, the following error message is displayed:

```
% A backup boot image must be set before setting a current boot image on USB storage device
```

In a VCStack configuration, the stack only accepts a release file on a USB storage device if a USB storage device is inserted in all stack members and all stack members have a bootloader version that supports booting from it. If a stack member has a USB storage device removed an error message is displayed. For example, if stack member 2 does not have a USB storage device inserted the following message is displayed:

```
% Stack member 2 has no USB storage device inserted
```

Examples To run the release file IE200-5.4.5I-01.rel stored on the device's Flash filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# boot system flash:/IE200-5.4.5I-01.rel
```

To remove the release file IE200-5.4.5I-01.rel stored on the device's Flash filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# no boot system flash:/IE200-5.4.5I-01.rel
```

To run the release file `IE200-5.4.5I-01.rel` stored on the switch's USB storage device filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# boot system usb:/IE200-5.4.5I-01.rel
```

To remove the release file `IE200-5.4.5I-01.rel` stored on the switch's USB storage device filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# boot system usb:/IE200-5.4.5I-01.rel
```

**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 remove the backup release file as the backup boot file.

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

Parameter	Description
<i><filepath-filename></i>	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.
backup	The specified file is a backup release file.

Mode Global Configuration

Examples To specify the file IE200-5.4.5I-01.rel as the backup to the main release file, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# boot system backup flash:/IE200-5.4.5I-01.rel
```

To remove the file IE200-5.4.5I-01.rel as the backup to the main release file, use the commands:

```
awplus# configure terminal
```

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

```
flash:/IE200-5.4.5I-01.rel
```

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 current-software

Overview This command copies the AlliedWare Plus™ OS software that the device has booted from, to a destination file. Specify whether the destination is Flash or USB when saving the software to the local filesystem.

Syntax `copy current-software <destination-name>`

Parameter	Description
<code><destination-name></code>	The filename and path where you would like the current running-release 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 103 for valid syntax.

Mode Privileged Exec

Example To copy the current software as installed in the working directory with the file name `my-release.rel`, use the command:

```
awplus# copy current-software my-release.rel
```

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

copy debug

Overview This command copies a specified debug file to a destination file. Specify whether the destination is Flash or USB when saving the software to the local filesystem.

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

Parameter	Description
<code><destination-name></code>	The filename and path where you would like the debug output saved. See Introduction on page 103 for valid syntax.
<code><source-name></code>	The filename and path where the debug output originates. See Introduction on page 103 for valid syntax.

Mode Privileged Exec

Example To copy debug output to a USB storage device with a filename my - debug, use the following command:

```
awplus# copy debug usb:mydebug
```

Output Figure 3-2: 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 103 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 103 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
<source-name>	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 103 for valid syntax.
<destination-name>	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 103 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 (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
- copy files stored on Flash memory to or from a different memory type, such as a USB storage device
- create two copies of the same file on your device

Syntax copy <source-name> <destination-name>

Parameter	Description
<source-name>	The filename and path of the source file. See Introduction on page 103 for valid syntax.
<destination-name>	The filename and path for the destination file. See Introduction on page 103 for valid syntax.

Mode Privileged Exec

Usage 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: all printable ASCII characters not included in the previous three categories. Including the following characters:
 - -
 - /
 - .
 - _
 - @
 - "
 - '
 - *
 - :
 - ~
 - ?

Do not use spaces or parentheses within filenames. Use hyphens or underlines instead.

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 `newconfig.cfg` onto your device's Flash from a USB storage device, use the command:

```
awplus# copy usb:/newconfig.cfg flash:/newconfig.cfg
```

To copy the file `newconfig.cfg` to a USB storage device from your device's Flash, use the command:

```
awplus# copy flash:/newconfig.cfg usb:/newconfig.cfg
```

To copy the file `config.cfg` into the current directory from a USB storage device, and rename it to `configtest.cfg`, use the command:

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

**Related
Commands** [copy zmodem](#)
[edit \(filename\)](#)
[show file systems](#)

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 103 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](#)

create autoboot

Overview Use this command to create an autoboot .txt file on external media. This command will automatically ensure that the keys and values that are expected in this file are correct. After the file is created the **create autoboot** command will copy the current release and configuration files across to the external media. The external media is then available to restore a release file and/or a configuration file to the device.

Syntax create autoboot [usb]

Mode Privileged Exec

Example To create an autoboot .txt file on external media, use the command:

```
awplus# create autoboot usb
```

**Related
Commands** [autoboot enable](#)
[show autoboot](#)
[show boot](#)

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 103 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
<source-name>	The filename and path where the debug output originates. See Introduction on page 103 for valid URL syntax.

Mode Privileged Exec

Example To delete debug output, use the following command:

```
awplus# delete debug
```

Output Figure 3-3: 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 no directory or file is specified then this command lists the files in the current working directory.

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

Parameter	Description
all	List all files.
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 no directory or file is specified, then this command lists the files in the current working directory.
debug	Debug root directory
flash	Flash memory root directory
nvs	NVS memory root directory
usb	USB storage device root directory

Mode Privileged Exec

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

```
awplus# dir
```

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

```
awplus# dir flash
```

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

```
awplus# dir all 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
```

**Related
Commands**

[cd](#)

[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 a filename is specified and it already exists, then the editor opens it in the text editor.

If no filename is specified, the editor prompts you for one when you exit it.

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.

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

Syntax edit [<filename>]

Parameter	Description
<filename>	Name of a file in the local Flash filesystem.

Mode Privileged Exec

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
```

Related Commands [edit \(filename\)](#)
[show file](#)

edit (filename)

Overview This command opens a remote text file as read-only in the AlliedWare Plus™ text editor.

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.

Syntax edit <filename>

Parameter	Description
<filename>	The filename and path of the remote file. See Introduction on page 103 for valid syntax.

Mode Privileged Exec

Usage 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: all printable ASCII characters not included in the previous three categories. Including the following characters:

- -
- /
- .
- _
- @
- "
- '
- *
- :
- ~
- ?

Do not use spaces or parentheses within filenames. Use hyphens or underlines instead.

Example To view the file bob . key stored in the security directory of a TFTP server, use the command:

```
awplus# edit tftp://security/bob.key
```

**Related
Commands**

- copy (filename)
- edit
- show file

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](#)

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 103 for valid syntax.
<code><destination-name></code>	The filename and path of the destination file. See Introduction on page 103 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|flash|nvs|usb}
{<source-name>|debug|flash|nvs|usb}`

Parameter	Description
<code><destination-name></code>	The filename and path where you would like the debug output moved to. See Introduction on page 103 for valid syntax.
<code><source-name></code>	The filename and path where the debug output originates. See Introduction on page 103 for valid syntax.

Mode Privileged Exec

Example To move debug output onto a USB storage device with a filename my - debug, use the following command:

```
awplus# move debug usb: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](#)

rmdir

Overview This command removes a directory. The directory must be empty for the command to work unless the optional **force** keyword is used to remove all subdirectories or files in a directory.

Syntax `rmdir [force] <name>`

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

Mode Privileged Exec

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

```
awplus# rmdir flash:/images
```

To force the removal of directory `level1` containing subdirectory `level2`, use the command:

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

**Related
Commands**

- `cd`
- `dir`
- `mkdir`
- `pwd`

show autoboot

Overview This command displays the Autoboot configuration and status.

Syntax show autoboot

Mode Privileged Exec

Example To show the Autoboot configuration and status, use the command:

```
awplus# show autoboot
```

Output Figure 3-5: Example output from the **show autoboot** command

```
awplus#show autoboot
Autoboot configuration
-----
Autoboot status           : enabled
USB file autoboot.txt exists : yes

Restore information on USB
Autoboot enable in autoboot.txt : yes
Restore release file       : IE200-5.4.5I-01.rel
(file exists)
Restore configuration file  : network_1.cfg (file exists)
```

Figure 3-6: Example output from the **show autoboot** command when an external media source is not present

```
awplus#show autoboot
Autoboot configuration
-----
Autoboot status           : disabled
External media source      : media not found.
```

Related Commands

- [autoboot enable](#)
- [create autoboot](#)
- [show boot](#)

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 3-7: Example output from the **show boot** command when the current boot config is on a USB storage device

```
awplus#show boot
Boot configuration
-----
Current software   : IE200-5.4.5I-01.rel
Current boot image : usb:/IE200-5.4.5I-01.rel
Backup boot image  : flash:/IE200-5.4.3A-1.3.rel
Default boot config: flash:/default.cfg
Current boot config: usb:/my.cfg (file exists)
Backup boot config: flash:/backup.cfg (file not found)
Autoboot status    : enabled
```

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

Parameter	Description
Current software	The current software release that the device is using.
Current boot image	The boot image currently configured for use during the next boot cycle.
Backup boot image	The boot image to use during the next boot cycle if the device cannot load the main image.
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**

- autoboot enable
- boot config-file backup
- boot system backup
- show autoboot

show file

Overview This command displays the contents of a specified file.

Syntax show file <filename>

Parameter	Description
<filename>	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](#)
- [edit \(filename\)](#)
- [show file systems](#)

show file systems

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

Syntax show file systems

Mode Privileged Exec

Examples To display the filesystems, use the command:

```
awplus# show file systems
```

Output Figure 3-8: 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
-----
 63.0M   8.2M   flash    rw    flash:    static local    Y
-        -     system   rw    system:    virtual local    -
 10.0M   9.9M   debug    rw    debug:    static local    Y
499.0K  430.0K nvs       rw    nvs:      static local    Y
-        -     usbstick rw    usb:      dynamic local    N
-        -     tftp      rw    tftp:     -         network -
-        -     scp        rw    scp:      -         network -
-        -     sftp       ro    sftp:     -         network -
-        -     http       ro    http:     -         network -
-        -     rsync      rw    rsync:    -         network -
```

Table 3-2: Parameters in the output of the **show file systems** command

Parameter	Description
Size (B) Available	The total memory available to this filesystem. The units are given after the value and are M for Megabytes or k for kilobytes.
Free (B)	The total memory free within this filesystem. The units are given after the value and are M for Megabytes or k for kilobytes.
Type	The memory type used for this filesystem; one of: flash system nvs tftp scp sftp http.
Flags	The file setting options: rw (read write), ro (read only).

Table 3-2: Parameters in the output of the **show file systems** command (cont.)

Parameter	Description
Prefixes	The prefixes used when entering commands to access the filesystems; one of: flash system nvs tftp scp sftp http.
S/V/D	The memory type: static, virtual, dynamic.
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](#)
- [edit \(filename\)](#)
- [show file](#)

show running-config

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

You can control the output in any one of the following ways:

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

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 running-config

Mode Privileged Exec and Global Configuration

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

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

Output Figure 3-9: Example output from the **show running-config** command

```
awplus#show running-config
!
service password-encryption
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$Jw0JGPr7YqoExA0GVasdE0
!
no service ssh
!
platform hwfilter-size ipv4-limited-ipv6
!
service telnet
no service telnet ipv6
!
service http
!
no clock timezone
!
no snmp-server ipv6
!
service test
!
aaa authentication enable default local
aaa authentication login default local
!
ip domain-lookup
!
!
!
no service dhcp-server
!
!
spanning-tree mode rstp
!
no ipv6 mld snooping
service power-inline
no spanning-tree rstp enable
!
interface port1.0.1-1.0.6
  switchport
  switchport mode access
!
interface vlan1
  shutdown
!
line con 0
!
end
```

Related [copy running-config](#)
Commands [show running-config access-list](#)

show running-config access-list

Overview Use this command to show the running system status and configuration details for access-list.

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 running-config access-list

Mode Privileged Exec and Global Configuration

Example To display the running system status and configuration details for access-list, use the command:

```
awplus# show running-config access-list
```

Output Figure 3-10: Example output from the **show running-config access-list** command

```
!  
access-list abc remark annai  
access-list abc deny any  
access-list abd deny any  
!
```

**Related
Commands** [copy running-config](#)
[show running-config](#)

show running-config dhcp

Overview Use this command to display the running configuration for DHCP server, DHCP snooping, and DHCP relay.

Syntax show running-config dhcp

Mode Privileged Exec and Global Configuration

Example To display to display the running configuration for DHCP server, DHCP snooping, and DHCP relay:

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

Output Figure 3-11: Example output from the **show running-config dhcp** command

```
!  
#show running-config dhcp  
no service dhcp-server  
!  
service dhcp-snooping  
!  
interface port1.0.1  
  ip dhcp snooping trust  
!  
interface port1.0.3  
  ip dhcp snooping max-bindings 25  
  access-group dhcpsnooping  
!  
interface port1.0.4  
  ip dhcp snooping max-bindings 25  
  access-group dhcpsnooping  
!  
interface po1  
  ip dhcp snooping max-bindings 25  
  arp security violation log  
!  
interface sa1  
  ip dhcp snooping max-bindings 25  
  access-group dhcpsnooping  
  arp security violation log  
!  
interface vlan100  
  ip dhcp snooping  
  arp security  
!  
interface vlan200  
  ip dhcp snooping  
  arp security  
!
```

**Related
Commands** [copy running-config](#)
[show running-config](#)

show running-config full

Overview Use this command to show the complete status and configuration of the running system.

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 running-config full

Mode Privileged Exec and Global Configuration

Example To display the complete status and configuration of the running system, use the command:

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

Output Figure 3-12: Example output from the **show running-config full** command

```
awplus#show running-config full
!
no service password-encryption
!
interface lo
ip address 127.0.0.1/8
ipv6 address ::1/128
!
interface vlan1
ip address 10.92.0.16/24
ipv6 address fe80::202:b3ff:fea1:2159/64
!
interface vlan2
ip address 20.10.10.54/24
ipv6 address fe80::200:5eff:fe00:101/64
ipv6 address fe80::202:b3ff:fea1:1567/64
ipv6 address fe80::204:76ff:fee6:6c1c/64
!
end
```

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

show running-config interface

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

Syntax `show running-config interface [<interface-list>] [dot1x|ip igmp|lacp|mstp|rstp|stp]`

Parameter	Description
<interface-list>	The interfaces or ports to display information about. An interface-list can be: • an interface (e.g. <code>vlan2</code>), a device port (e.g. <code>port1.0.4</code>), a static channel group (e.g. <code>sa2</code>) or a dynamic (LACP) channel group (e.g. <code>po2</code>) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen, e.g. <code>vlan2-8</code>, or <code>port1.0.1-1.0.4</code>, or <code>sa1-2</code>, or <code>po1-2</code> • a comma-separated list of the above, e.g. <code>port1.0.1, port1.0.4-1.0.6</code>. Do not mix interface types in a list The specified interfaces must exist.
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.
mstp	Displays running configuration for MSTP (Multiple Spanning Tree Protocol) 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

Examples To display the current running configuration of your device for ports 1 to 4, use the command:

```
awplus# show running-config interface port1.0.1-port1.0.4
```

To display the current running configuration of a device for VLAN 1, use the command:

```
awplus# show running-config interface vlan1
```

To display the current running configuration of a device for VLANs 1 and 3-5, use the command:

```
awplus# show running-config interface vlan1,vlan3-vlan5
```

Output Figure 3-13: Example output from a **show running-config interface** port1.0.2 command

```
awplus#sh running-config interface port1.0.2
!
interface port1.0.2
  switchport
  switchport mode access
!
```

Figure 3-14: Example output from the **show running-config interface** command

```
awplus#sh running-config interface
interface port1.0.1-1.0.6
  switchport
  switchport mode access
!
interface vlan1
  ip address 192.168.1.1/24
  ip rip authentication mode md5
  ip rip authentication string mykey
  ip irdp
!
interface vlan2
  ip address 192.168.2.2/24
  ip rip authentication mode md5
  ip rip authentication key-chain cars
!
```

**Related
Commands** [copy running-config](#)
[show running-config](#)

show running-config ipv6 access-list

Overview Use this command to show the running system status and configuration for IPv6 ACLs.

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 running-config ipv6 access-list

Mode Privileged Exec and Global Configuration

Example To display the running system status and configuration for IPv6 ACLs, use the command:

```
awplus# show running-config ipv6 access-list
```

Output Figure 3-15: Example output from the **show running-config ipv6 access-list** command

```
!  
ipv6 access-list abc permit any  
!
```

**Related
Commands** [copy running-config](#)
[show running-config](#)

show running-config key chain

Overview Use this command to show the running system key-chain related configuration.

Syntax show running-config key chain

Mode Privileged Exec and Global Configuration

Example To display the running system key-chain related configuration, use the command:

```
awplus# show running-config key chain
```

Output Figure 3-16: Example output from the **show running-config key chain** command

```
!
key chain 12
key 2
key-string 234
!
key chain 123
key 3
key-string 345
!
```

**Related
Commands** [copy running-config](#)
[show running-config](#)

show running-config lldp

Overview This command shows the current running configuration of LLDP.

Syntax show running-config lldp

Mode Privileged Exec and Global Configuration

Example To display the current configuration of LLDP, use the command:

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

Output Figure 3-17: Example output from the **show running-config lldp** command

```
awplus#show running-config lldp

lldp notification-interval 10
lldp timer 20
!
interface port1.0.1
  lldp notifications
  lldp tlv-select port-description
  lldp tlv-select system-name
  lldp tlv-select system-description
  lldp tlv-select management-address
  lldp transmit receive
```

**Related
Commands** [show lldp](#)
[show lldp interface](#)

show running-config power-inline

Overview Use this command to show the Power over Ethernet (PoE) running system status and configuration details. The PoE usage-threshold percentage as specified by the [power-inline usage-threshold](#) command is displayed in the **running-config** using this command.

Syntax show running-config power-inline

Mode Privileged Exec and Global Configuration

Example To display the PoE running system status and configuration details, use the command:

```
awplus# show running-config power-inline
```

Output Figure 3-18: Example output from the **show running-config power-inline** command

```
!  
power-inline usage-threshold 90  
!
```

Related Commands [power-inline usage-threshold](#)
[show power-inline](#)

show running-config router-id

Overview Use this command to show the running system global router ID configuration.

Syntax show running-config router-id

Mode Privileged Exec and Global Configuration

Example To display the running system global router ID configuration, use the command:

```
awplus# show running-config router-id
```

Output Figure 3-19: Example output from the **show running-config router-id** command

```
!  
router-id 3.3.3.3  
!
```

**Related
Commands** [copy running-config](#)
[show running-config](#)

show running-config security-password

Overview This command displays the configuration settings for the various security-password rules. If a default parameter is used for a security-password rule, therefore disabling that rule, no output is displayed for that feature.

Syntax show running-config security-password

Mode Privileged Exec and Global Configuration

Example To display the current security-password rule settings in the running-config, use the command:

```
awplus# show running-config security-password
```

Output Figure 3-20: Example output from the **show running-config security-password** command

```
security-password minimum-length 8
security-password minimum-categories 3
security-password history 4
security-password lifetime 30
security-password warning 3
security-password forced-change
```

Related Commands [show security-password configuration](#)
[show security-password user](#)

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 “Controlling “show” Command Output” in 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 3-21: Example output from the **show startup-config** command

```
awplus#show startup-config
!
service password-encryption
!
username manager privilege 15 password 8 $1$bJoVec4D$Jw0JGPr7YqoExA0GVasdE0
!
no service ssh
!
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](#)

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

System Configuration and Monitoring Commands

Introduction

Overview This chapter provides an alphabetical reference of commands for configuring and monitoring the system.

- Command List**
- ["banner exec"](#) on page 162
 - ["banner login \(system\)"](#) on page 164
 - ["banner motd"](#) on page 166
 - ["clock set"](#) on page 168
 - ["clock summer-time date"](#) on page 169
 - ["clock summer-time recurring"](#) on page 171
 - ["clock timezone"](#) on page 173
 - ["continuous-reboot-prevention"](#) on page 174
 - ["ecofriendly led"](#) on page 176
 - ["findme"](#) on page 177
 - ["hostname"](#) on page 178
 - ["no debug all"](#) on page 180
 - ["reboot"](#) on page 181
 - ["reload"](#) on page 182
 - ["show clock"](#) on page 183
 - ["show continuous-reboot-prevention"](#) on page 185
 - ["show cpu"](#) on page 186
 - ["show cpu history"](#) on page 189
 - ["show debugging"](#) on page 192
 - ["show ecofriendly"](#) on page 193

- [“show interface memory”](#) on page 194
- [“show memory”](#) on page 196
- [“show memory allocations”](#) on page 198
- [“show memory history”](#) on page 200
- [“show memory pools”](#) on page 201
- [“show memory shared”](#) on page 202
- [“show process”](#) on page 203
- [“show reboot history”](#) on page 205
- [“show router-id”](#) on page 206
- [“show system”](#) on page 207
- [“show system environment”](#) on page 208
- [“show system interrupts”](#) on page 209
- [“show system mac”](#) on page 210
- [“show system pluggable”](#) on page 211
- [“show system pluggable detail”](#) on page 213
- [“show system pluggable diagnostics”](#) on page 217
- [“show system serialnumber”](#) on page 219
- [“show tech-support”](#) on page 220
- [“speed \(asyn\)”](#) on page 222
- [“system territory \(deprecated\)”](#) on page 224
- [“terminal monitor”](#) on page 225
- [“undebg all”](#) on page 226

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) 5.4.5 06/06/14 00:44:25
```

Mode Global Configuration

Examples To configure a User Exec mode banner after login, enter the following commands:

```
awplus#configure terminal
awplus(config)#banner exec enable to move to Priv Exec mode
awplus(config)#exit
awplus#exit
awplus login: manager
Password:
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) 5.4.5 06/06/14
13:03:59
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 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 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) 5.4.5 06/06/14
13:03:59
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:
awplus>
```

**Related
Commands** [banner exec](#)
 [banner motd](#)

banner motd

Overview Use this command to change 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 not display a text MOTD (Message-of-the-Day) banner on login.

Syntax banner motd <*motd-text*>
no banner motd

Default By default, the device displays the AlliedWare Plus™ OS version and build date before login.

Mode Global Configuration

Examples To configure a MOTD banner to be displayed when you log in, enter the following commands:

```
awplus>enable
awplus#configure terminal
awplus(config)#banner motd system shutdown at 6pm
awplus(config)#exit
awplus#exit
system shutdown at 6pm

awplus login: manager
Password:

AlliedWare Plus (TM) 5.4.5 06/06/14
13:03:59
```

To remove the login banner, enter the following commands:

```
awplus>enable
awplus#configure terminal
awplus(config)#no banner motd
awplus(config)#exit
awplus#exit
awplus login: manager
Password:
AlliedWare Plus (TM) 5.4.5 06/06/14
13:03:59
awplus>
```

**Related
Commands** [banner exec](#)
[banner login \(system\)](#)

clock set

Overview This command sets the time and date for the system clock.

Syntax clock set <hh:mm:ss> <day> <month> <year>

Parameter	Description
<hh:mm:ss>	Local time in 24-hour format
<day>	Day of the current month <1-31>
<month>	The first three letters of the current month.
<year>	Current year <2000-2035>

Mode Privileged Exec

Usage Configure the timezone before setting the local time. Otherwise, when you change the timezone, the device applies the new offset to the local time.

NOTE: If Network Time Protocol (NTP) is enabled, then you cannot change the time or date using this command. NTP maintains the clock automatically using an external time source. If you wish to manually alter the time or date, you must first disable NTP.

Example To set the time and date on your system to 2pm on the 2nd of April 2007, use the command:

```
awplus# clock set 14:00:00 2 apr 2007
```

Related Commands [clock timezone](#)

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, in the range 1-31.
<start-month>	First three letters of the name of the month that the summertime starts.
<start-year>	Year that summertime starts, in the range 2000-2035.
<start-time>	Time of the day that summertime starts, in the 24-hour time format HH:MM.
<end-day>	Day that summertime ends, in the range 1-31.
<end-month>	First three letters of the name of the month that the summertime ends.
<end-year>	Year that summertime ends, in the range 2000-2035.
<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 1st October 2007 and end on the 18th of March 2008:

```
awplus(config)# clock summer-time NZDT date 1 oct 2:00 2007 18  
mar 2:00 2008 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 1st Sunday in October, and end on the 3rd Sunday in March, use the command:

```
awplus(config)# clock summer-time NZDT recurring 1 sun oct 2:00  
3 sun mar 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.
minus or plus	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 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 set](#)
[clock summer-time date](#)
[clock summer-time recurring](#)

continuous-reboot-prevention

Overview Use this command to enable and to configure the continuous reboot prevention feature. Continuous reboot prevention allows the user to configure the time period during which reboot events are counted, the maximum number of times the switch can reboot within the specified time period, referred to as the threshold, and the action to take if the threshold is exceeded.

This command is available with Software Version 5.4.3A-1.x and later.

Use the **no** variant of this command to disable the continuous reboot prevention feature or to return the **period**, **threshold** and **action** parameters to the defaults.

Syntax `continuous-reboot-prevention enable`
`continuous-reboot-prevention [period <0-604800>] [threshold <1-10>] [action [linkdown|logonly|stopreboot]]`
`no continuous-reboot-prevention enable`
`no continuous-reboot-prevention [period] [threshold] [action]}`

Parameter	Description
enable	Enable the continuous reboot prevention feature.
period	Set the period of time in which reboot events are counted. <0-604800> Period value in seconds. The default is 600.
threshold	Set the maximum number of reboot events allowed in the specified period. <1-10> Threshold value. The default is 1.
action	Set the action taken if the threshold is exceeded. linkdown Reboot procedure continues and all switch ports and stack ports stay link-down. The reboot event is logged. This is the default action. logonly Reboot procedure continues normally and the reboot event is logged. stopreboot Reboot procedure stops until the user enters the key "c" via the CLI. Normal reboot procedure then continues and the reboot event is logged.

Default Continuous reboot prevention is disabled by default. The default period value is 600, the default threshold value is 1 and the default action is linkdown.

Mode Global Configuration

Usage Note that user initiated reboots via the CLI, and software version auto-synchronization reboots, are not counted toward the threshold value.

Examples To enable continuous reboot prevention, use the commands:

```
awplus# configure terminal
awplus(config)# continuous-reboot-prevention enable
```

To set the period to 500 and action to stopreboot, use the commands:

```
awplus# configure terminal
awplus(config)# continuous-reboot-prevention period 500 action
stopreboot
```

To return the period and action to the defaults and keep the continuous reboot prevention feature enabled, use the commands:

```
awplus# configure terminal
awplus(config)# no continuous-reboot-prevention period action
```

To disable continuous reboot prevention, use the commands:

```
awplus# configure terminal
awplus(config)# no continuous-reboot-prevention enable
```

**Related
Commands** [show continuous-reboot-prevention](#)
[show reboot history](#)
[show tech-support](#)

ecofriendly led

Overview Use this command to enable the eco-friendly LED (Light Emitting Diode) feature, which turns off power to the port LEDs. Power to the system status LED is not disabled.

Use the **no** variant of this command to disable the eco-friendly LED feature.

Syntax ecofriendly led
no ecofriendly led

Default The eco-friendly LED feature is disabled by default.

Mode Global Configuration

Usage When the eco-friendly LED feature is enabled, a change in port status will not affect the display of the associated LED. When the eco-friendly LED feature is disabled and power is returned to port LEDs, the LEDs will correctly show the current state of the ports.

For an example of how to configure a trigger to turn off power to port LEDs, see the [Triggers Feature Overview and Configuration Guide](#).

Examples To enable the eco-friendly LED feature which turns off power to all port LEDs, use the following commands:

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

To disable the eco-friendly LED feature, use the following command:

```
awplus# configure terminal
awplus(config)# no ecofriendly led
```


findme

Overview Use this command to physically locate a specific device from a group of similar devices. Activating the command causes a selected number of port LEDs to alternately flash green then amber (if that device has amber LEDs) at a rate of 1 Hz.

Use the **no** variant of this command to deactivate the Find Me feature prior to the timeout expiring.

Syntax no findme

Parameter	Description
<port - list>	The ports to flash. The port list can be: • a switch port, e.g. port1.0.4 • a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.4 • a comma-separated list of ports and port ranges, e.g. port1.0.1, port1.0.5-1.0.6.
<duration>	Specify the duration in seconds within the range of 5-3600 seconds.

Default By default all port LEDs flash for 60 seconds.

Mode Privileged Exec

Usage Running the **findme** command causes the device's port LEDs to flash. An optional **timeout** parameter specifies the flash behavior duration. Normal LED behavior is restored automatically after either the default time, or a specified time has elapsed, or a **no findme** command is used. You can specify which interface or interfaces are flashed with the optional **interface** parameter.

Example To activate the Find Me feature for the default duration (60 seconds) on all ports, use the following command:

```
awplus# findme
```

To activate the Find Me feature for 120 seconds on all ports, use the following command:

```
awplus# findme timeout 120
```

To activate the Find Me feature for the default duration (60 seconds) on switch port interfaces port1.0.2 through port1.0.4, use the following command:

```
awplus# findme interface port1.0.2-1.0.4
```

In the example above, ports 2 to 4 will flash 4 times and then all ports will flash twice. Each alternate flash will be amber (if that device has amber LEDs). This pattern will repeat until **timeout** (default or set) or **no findme** commands are used.

To deactivate the Find Me feature, use the following command:

```
awplus# no findme
```

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 (awplus).

Syntax hostname <hostname>
no hostname [<hostname>]

Parameter	Description
<hostname>	Specifies the name given to a specific device. Also referred to as the Node Name in AMF output screens.

Default awplus

Mode Global Configuration

Usage 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.

NOTE: Within an AMF network, any device without a hostname applied 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 accordingly apply an appropriate hostname to each device.

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](#)

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.

The debugging facility is disabled by default.

Syntax no debug all [dot1x|ipv6|nsm]

Parameter	Description
dot1x	Turns off all debugging for IEEE 802.1X port-based network access-control.
ipv6	Turns off all debugging for IPv6 (Internet Protocol version 6).
nsm	Turns off all debugging for the NSM (Network Services Module).

Mode Global Configuration and Privileged Exec

Example To disable debugging for all features, use the command:

```
awplus# no debug all
```

To disable all 802.1X debugging, use the command:

```
awplus# no debug all
```

To disable all IPv6 debugging, use the command:

```
awplus# no debug all
```

To disable all NSM debugging, use the command:

```
awplus# no debug all
```

Related Commands [undebug all](#)

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 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 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 4-1: Example output from the **show clock** command for a device using New Zealand time

```
Local Time: Mon,  6 Aug 2007 13:56:06 +1200
UTC Time:  Mon,  6 Aug 2007 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 4-1: 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 set](#)
- [clock summer-time date](#)
- [clock summer-time recurring](#)
- [clock timezone](#)

show continuous-reboot-prevention

Overview This command displays the current continuous reboot prevention configuration.

Syntax show continuous-reboot-prevention

Mode User Exec and Privileged Exec

Examples To show the current continuous reboot prevention configuration, use the command:

```
awplus# show continuous-reboot-prevention
```

Output Figure 4-2: Example output from the **show continuous-reboot-prevention** command

```
-----  
Continuous reboot prevention  
-----  
status=disabled  
period=600  
threshold=1  
action=linkdown  
-----
```

Related Commands [continuous-reboot-prevention](#)
[show reboot history](#)

show cpu

Overview This command displays a list of running processes with their CPU utilization. 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 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 4-3: Example output from the **show cpu** command

```
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 4-2: 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.

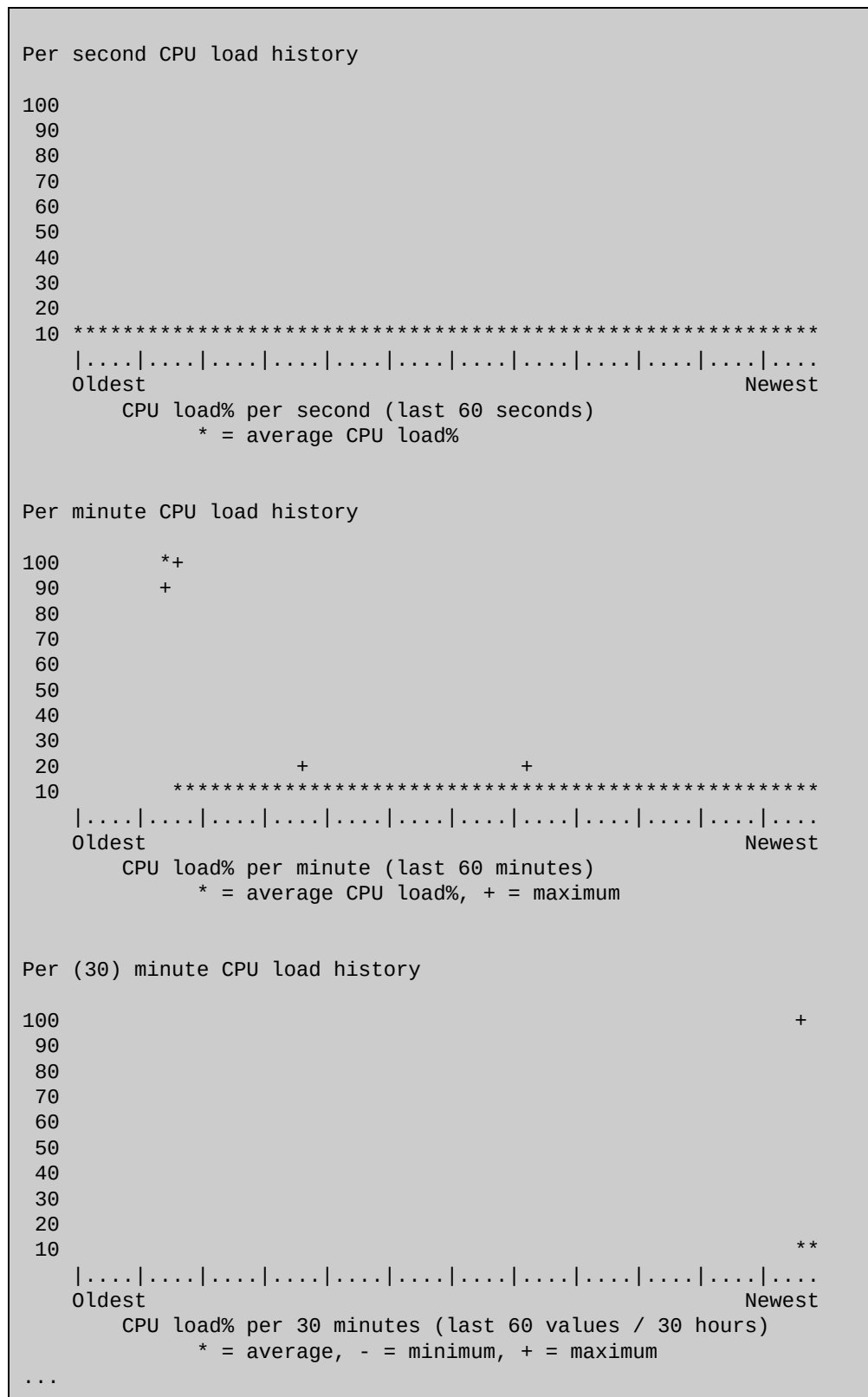
Related Commands

- [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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).
- Syntax** show cpu history
- Mode** User Exec and Privileged Exec
- Usage** 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 4-4: 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 information for all debugging options.  
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 debugging
- Default** This command runs all the **show debugging** commands in alphabetical order.
- Mode** User Exec and Privileged Exec
- Usage** This command displays all debugging information, similar to the way the [show tech-support](#) command displays all show output for use by Allied Telesis authorized service personnel only.
- Example** To display all debugging information, use the command:  
awplus# show debugging
- Output** Figure 4-5: Example output from the **show debugging** command

```
awplus#show debugging
AAA debugging status:
 Authentication debugging is off
 Accounting debugging is off

% DHCP Snooping service is disabled

802.1X debugging status:

EPSR debugging status:
 EPSR Info debugging is off
 EPSR Message debugging is off
 EPSR Packet debugging is off
 EPSR State debugging is off

IGMP Debugging status:
 IGMP Decoder debugging is off
 IGMP Encoder debugging is off
...
```



# show ecofriendly

**Overview** This command displays the switch's eco-friendly configuration status. The [ecofriendly led](#) configuration status are shown in the [show ecofriendly](#) output.

**Syntax** show ecofriendly

**Mode** Privileged Exec and Global Configuration

**Example** To display the switch's eco-friendly configuration status, use the following command:

```
awplus# show ecofriendly
```

**Output** Figure 4-6: Example output from the **show ecofriendly** command

```
awplus#show ecofriendly
Front panel port LEDs normal

Energy efficient ethernet
Port Name Configured Status
port1.0.1 Port 1 off -
port1.0.2 off off
port1.0.3 off -
port1.0.4 Port 4 off -
port1.0.5 off -
...
```

Table 4-3: Parameters in the output of the **show ecofriendly** command

| Parameter  | Description                                                                                                              |
|------------|--------------------------------------------------------------------------------------------------------------------------|
| normal     | The eco-friendly LED feature is disabled and port LEDs show the current state of the ports. This is the default setting. |
| off        | The eco-friendly LED feature is enabled and power to the port LEDs is disabled.                                          |
| Port       | Displays the port number as assigned by the switch.                                                                      |
| Name       | Displays the port name if a name is configured for a port number.                                                        |
| Configured | Because LPI is not supported, this entry always shows "off" or a dash (-).                                               |
| Status     | Because LPI is not supported, this entry always shows "off" or a dash (-).                                               |

# show interface memory

**Overview** This command displays the shared memory used by either all interfaces, or the specified interface or interfaces. The output is useful for diagnostic purposes by Allied Telesis authorized service personnel.

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 interface memory  
show interface <port-list> memory

| Parameter   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <port-list> | The ports to display information about. The port list can be: <ul style="list-style-type: none"><li>• a switch port (e.g. port1.0.4) a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of ports and port ranges, e.g. port1.0.1, port1.0.4-1.0.6. Do not mix switch ports, static channel groups, and dynamic (LACP) channel groups in the same list</li></ul> |

**Mode** User Exec and Privileged Exec

**Example** To display the shared memory used by all interfaces, use the command:  
awplus# show interface memory  
To display the shared memory used by port1.0.1 and port1.0.5 to port1.0.6, use the command:

```
awplus# show interface port1.0.1,port1.0.5-1.0.6 memory
```

**Output** Figure 4-7: Example output from the **show interface <port-list> memory** command

|                                                        |        |            |        |        |  |
|--------------------------------------------------------|--------|------------|--------|--------|--|
| awplus#show interface port1.0.1,port1.0.5-1.0.6 memory |        |            |        |        |  |
| Vlan blocking state shared memory usage                |        |            |        |        |  |
| -----                                                  |        |            |        |        |  |
| Interface                                              | shmid  | Bytes Used | nattch | Status |  |
| port1.0.1                                              | 393228 | 512        | 1      |        |  |
| port1.0.5                                              | 491535 | 512        | 1      |        |  |
| port1.0.6                                              | 557073 | 512        | 1      |        |  |

Figure 4-8: Example output from the **show interface memory** command

```
awplus#show interface memory
Vlan blocking state shared memory usage

```

| Interface  | shmid   | Bytes | Used | nattch | Status |
|------------|---------|-------|------|--------|--------|
| port1.0.1  | 393228  | 512   |      | 1      |        |
| port1.0.2  | 458766  | 512   |      | 1      |        |
| port1.0.3  | 360459  | 512   |      | 1      |        |
| port1.0.4  | 524304  | 512   |      | 1      |        |
| port1.0.5  | 491535  | 512   |      | 1      |        |
| port1.0.6  | 557073  | 512   |      | 1      |        |
| port1.0.7  | 327690  | 512   |      | 1      |        |
| port1.0.8  | 655380  | 512   |      | 1      |        |
| port1.0.9  | 622611  | 512   |      | 1      |        |
| ...        |         |       |      |        |        |
| port1.0.21 | 950301  | 512   |      | 1      |        |
| port1.0.22 | 1048608 | 512   |      | 1      |        |
| port1.0.23 | 1015839 | 512   |      | 1      |        |
| port1.0.24 | 1081377 | 512   |      | 1      |        |
| lo         | 425997  | 512   |      | 1      |        |
| po1        | 1179684 | 512   |      | 1      |        |
| po2        | 1212453 | 512   |      | 1      |        |
| sa3        | 1245222 | 512   |      | 1      |        |

**Related** [show interface brief](#)  
**Commands** [show interface status](#)  
[show interface switchport](#)

# 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**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 amount of memory the process is currently using.                                                                               |
| 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 4-9: Example output from the **show memory** command

```
awplus#show memory sort stk
```

|                                                         |          |      |          |          |          |         |          |
|---------------------------------------------------------|----------|------|----------|----------|----------|---------|----------|
| RAM total: 124384 kB; free: 64236 kB; buffers: 15888 kB |          |      |          |          |          |         |          |
| user processes                                          |          |      |          |          |          |         |          |
| =====                                                   |          |      |          |          |          |         |          |
| pid                                                     | name     | mem% | size(kB) | peak(kB) | data(kB) | stk(kB) | virt(kB) |
| 490                                                     | openhpid | 1.5  | 1988     | 7480     | 1308     | 528     | 6704     |
| 578                                                     | hsl      | 7.1  | 8940     | 29312    | 5148     | 312     | 21052    |
| 18986                                                   | imish    | 1.3  | 1660     | 13668    | 3876     | 172     | 13668    |
| 18931                                                   | imish    | 3.6  | 4548     | 13668    | 3876     | 172     | 13668    |
| 576                                                     | imi      | 4.6  | 5772     | 14532    | 4428     | 144     | 14532    |
| 572                                                     | nsm      | 4.9  | 6128     | 15092    | 4480     | 140     | 15092    |
| 574                                                     | hostd    | 1.6  | 2048     | 8116     | 1876     | 140     | 8116     |
| 586                                                     | cntrd    | 2.5  | 3168     | 12140    | 3288     | 140     | 12136    |
| 606                                                     | sflowd   | 2.8  | 3564     | 12336    | 3408     | 140     | 12336    |
| 610                                                     | authd    | 3.0  | 3808     | 12604    | 3472     | 140     | 12604    |
| 616                                                     | mstp     | 3.1  | 3856     | 12652    | 3480     | 140     | 12652    |
| ...                                                     |          |      |          |          |          |         |          |

Table 4-4: 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.                                  |

**Related  
Commands**

[show memory allocations](#)  
[show memory history](#)  
[show memory pools](#)  
[show memory shared](#)

# show memory allocations

**Overview** This command displays the memory allocations used by processes.

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 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 4-10: 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show memory history

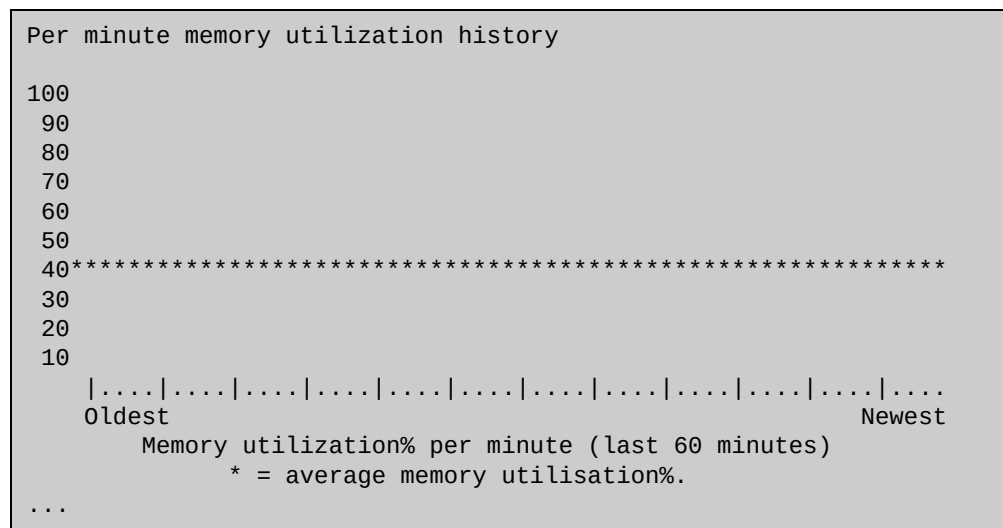
**Mode** User Exec and Privileged Exec

**Usage** 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 4-11: 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 “Controlling “show” Command Output” in 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 shows the memory pools used by processes, use the command:

```
awplus# show memory pools
```

**Output** Figure 4-12: 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 “Controlling “show” Command Output” in 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 4-13: 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 “Controlling “show” Command Output” in 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

**Example** To display a summary of the current running processes, use the command:

```
awplus# show process
```

**Output** Figure 4-14: Example output from the **show process** command

```

CPU load for 1 minute: 0%; 5 minutes: 3%; 15 minutes: 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 4-5: Parameters in the output from the **show process** command

| Parameter | Description                                                        |
|-----------|--------------------------------------------------------------------|
| CPU load  | Average CPU load for the given period.                             |
| 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.  
The history is stored in NVS memory, so it will be lost after a power cycle.
- 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 4-15: Example output from the **show reboot history** command

```
awplus#show
reboot history
```

| <date>     | <time>   | <type>     | <description>                                            |
|------------|----------|------------|----------------------------------------------------------|
| 2014-01-10 | 01:42:04 | Expected   | User Request                                             |
| 2014-01-10 | 01:35:31 | Expected   | User Request                                             |
| 2014-01-10 | 01:16:25 | Unexpected | Rebooting due to critical process (network/nsm) failure! |
| 2014-01-10 | 01:11:04 | Unexpected | Rebooting due to critical process (network/nsm) failure! |
| 2014-01-09 | 19:56:16 | Expected   | User Request                                             |
| 2014-01-09 | 19:51:20 | Expected   | User Request                                             |

Table 4-6: Parameters in the output from the **show reboot history** command

| Parameter                    | Description                                                                                                                                                                                                                 |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Unexpected                   | Reboot is counted by the continuous reboot prevention feature if the reboot event occurs in the time period specified for continuous reboot prevention.                                                                     |
| Expected                     | Reboot is not counted by continuous reboot prevention feature.                                                                                                                                                              |
| Continuous reboot prevention | A continuous reboot prevention event has occurred. The action taken is configured with the <b>continuous-reboot-prevention</b> command. The next time period during which reboot events are counted begins from this event. |
| User request                 | User initiated reboot via the CLI.                                                                                                                                                                                          |

- Related Commands** [show continuous-reboot-prevention](#)  
[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 4-16: Example output from the **show router-id** command

```
awplus>show router-id
Router ID: 10.55.0.2 (automatic)
```

# show system

**Overview** This command displays general system information about the device, including the hardware installed, memory, and software versions loaded. It also displays location and contact details when these have been set.

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 system

**Mode** User Exec and Privileged Exec

**Example** To display configuration information, use the command:

```
awplus# show system
```

**Output** Figure 4-17: Example output from the **show system** command

```
awplus#show system
Switch System Status Sun Jan 03 00:04:33 2010

Board ID Bay Board Name Rev Serial number

Base 410 at-IE200-6GP X1-0 NONE

RAM: Total: 252888 kB Free: 144744 kB
Flash: 63.0MB Used: 54.8MB Available: 8.2MB

Environment Status : Normal
Uptime : 0 days 00:08:53
Bootloader version : 3.0.0-devel/1.0_20
Current software : IE200-5.4.5I-01.rel
Software version : 5.4.3A
Build date : Tue Apr 29 10:38:19 NZST 2014
Current boot config: flash:/default.cfg (file exists)
System Name
 awplus
System Contact
System Location
```

**Related Commands** [show system environment](#)

# show system environment

**Overview** This command displays the current environmental status of your device and any attached PSU, XEM, or other expansion option. The environmental status covers information about temperatures, fans, and voltage.

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 system environment

**Mode** User Exec and Privileged Exec

**Example** To display the system’s environmental status, use the command:

```
awplus# show system environment
```

**Output** Figure 4-18: Example output from the **show system environment** command

```
awplus#show system environment
Environment Monitoring Status
Overall Status: Normal

Resource ID: 1 Name: at-IE200-6GP
ID Sensor (Units) Reading Low Limit High Limit Status
1 Almon: LED output (Bit) 0 0 0 Ok
2 Almon: relay output (Bit) 0 0 0 Ok
3 Temp: Local (Degrees C) 58 85(Hyst) 95 Ok
4 Contact Input 1 Yes - - Ok
5 Relay Output 1 Yes - - Ok
6 PSU Power Output 1 Yes - - Ok
7 PSU Power Output 2 No - - Ok
```

**Related Commands** [show system](#)



# show system interrupts

**Overview** Use this command to display the number of interrupts for each IRQ (Interrupt Request) used to interrupt input lines on a PIC (Programmable Interrupt Controller) on your 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 system interrupts

**Mode** User Exec and Privileged Exec

**Example** To display information about the number of interrupts for each IRQ in your device, use the command:

```
awplus# show system interrupts
```

**Related Commands** [show system environment](#)

# 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 4-19: Example output from the **show system mac** command

```
awplus#show system mac
eccd.6d9d.4eed
```

# show system pluggable

**Overview** This command displays **brief** pluggable transceiver information showing the pluggable type, the pluggable serial number, and the pluggable port on the device. Different types of pluggable transceivers are supported in different models of device. See your Allied Telesis dealer for more information about the models of pluggables that your device supports.

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 system pluggable [*<port-list>*]

| Parameter                | Description                                                                                                                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | The ports to display information about. The port list can be: <ul style="list-style-type: none"><li>• a switch port (e.g. port1.0.6)</li><li>• a continuous range of ports separated by a hyphen, e.g. port1.0.5-1.0.6</li><li>• a comma-separated list of ports and port ranges, e.g. port1.0.5, port1.0.6.</li></ul> |

**Mode** User Exec and Privileged Exec

**Example** To display brief information about all installed pluggable transceivers, use the command:

```
awplus# show system pluggable
```

**Output** Figure 4-20: Example output from the **show system pluggable** command

| awplus#show system pluggable |        |                 |                  |          |           |
|------------------------------|--------|-----------------|------------------|----------|-----------|
| System Pluggable Information |        |                 |                  |          |           |
| Port                         | Vendor | Device          | Serial Number    | Datecode | Type      |
| 1.0.5                        | ATI    | AT-TN-P015-A    | A04840R131700049 | 130422   | BASE-BX10 |
| 1.0.6                        | ATI    | AT-SPFXBD-LC-15 | A03947R074700751 | 07112601 | BASE-BX10 |

**Example** To display information about the pluggable transceiver installed in port1.0.5, use the command:

```
awplus# show system pluggable port1.0.5
```

**Output** Figure 4-21: Example output from the **show system pluggable port1.0.5** command

| System Pluggable Information |              |              |                  |          |           |
|------------------------------|--------------|--------------|------------------|----------|-----------|
| Port                         | Manufacturer | Device       | Serial Number    | Datecode | Type      |
| 1.0.5                        | ATI          | AT-TN-P015-A | A04840R131700049 | 130422   | BASE-BX10 |

**Related Commands**

- [show system environment](#)
- [show system pluggable detail](#)
- [show system pluggable diagnostics](#)

# show system pluggable detail

**Overview** This command displays detailed pluggable transceiver information showing the pluggable type, the pluggable serial number, and the pluggable port on the device. Different types of pluggable transceivers are supported in different models of device. See your Allied Telesis dealer for more information about the models of pluggables that your device supports.

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 system pluggable [*<port-list>*] detail

| Parameter                | Description                                                                                                                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | The ports to display information about. The port list can be: <ul style="list-style-type: none"><li>• a switch port (e.g. port1.0.6)</li><li>• a continuous range of ports separated by a hyphen, e.g. port1.0.5-1.0.6</li><li>• a comma-separated list of ports and port ranges, e.g. port1.0.5, port1.0.6.</li></ul> |

**Mode** User Exec and Privileged Exec

In addition to the information about pluggable transceivers displayed using the [show system pluggable](#) command (port, manufacturer, serial number, manufacturing datecode, and type information), the **show system pluggable detail** command displays the following information:

- **SFP Laser Wavelength:** Specifies the laser wavelength of the installed pluggable transceiver
- **Single mode Fiber:** Specifies the link length supported by the pluggable transceiver using single mode fiber
- **OM1 (62.5μ m) Fiber:** Specifies the link length (in μm - micron) supported by the pluggable transceiver using 62.5 micron multi-mode fiber.
- **OM2 (50μ m) Fiber:** Specifies the link length (in μm - micron) supported by the pluggable transceiver using 50 micron multi-mode fiber.
- **Diagnostic Calibration:** Specifies whether the pluggable transceiver supports DDM or DOM Internal or External Calibration.
  - **Internal** is displayed if the pluggable transceiver supports DDM or DOM Internal Calibration.
  - **External** is displayed if the pluggable transceiver supports DDM or DOM External Calibration.
  - - is displayed if SFP DDM Internal Calibration or External Calibration is not supported.

- **Power Monitoring:** Displays the received power measurement type, which can be either **OMA**(Optical Module Amplitude) or **Avg**(Average Power) measured in  $\mu$ W.

**NOTE:** For parameters that are not supported or not specified, a hyphen is displayed instead.

**Example** To display detailed information about the pluggable transceivers installed in a particular port on the device, use a command like:

```
awplus# show system pluggable port1.0.4 detail
```

To display detailed information about all the pluggable transceivers installed on the device, use the command:

```
awplus# show system pluggable detail
```

**Output** Figure 4-22: Example output from the **show system pluggable detail** command on a device

```
awplus#show system pluggable detail
System Pluggable Information Detail
Port1.0.5
=====
Vendor Name: ATI
Device Name: AT-SPTX
Device Type: 1000BASE-T
Serial Number: A123459071900003
Manufacturing Datecode: 07051101
SFP Laser Wavelength: -
Link Length Supported
 Single Mode Fiber : -
 OM1 (62.5um) Fiber: -
 OM2 (50um) Fiber : -
Diagnostic Calibration: -
Power Monitoring: -
FEC BER support: -

Port1.0.6
=====
Vendor Name: ATI
Device Name: AT-SPBD10-13
Device Type: BASE-BX10
Serial Number: A03243R111300129
Manufacturing Datecode: 11032801
SFP Laser Wavelength: 1310nm
Link Length Supported
 Single Mode Fiber : 10Km
 OM1 (62.5um) Fiber: -
 OM2 (50um) Fiber : -
Diagnostic Calibration: -
Power Monitoring: -
FEC BER support: -
```

Table 4-7: Parameters in the output from the **show system pluggables detail** command:

| Parameter     | Description                                                          |
|---------------|----------------------------------------------------------------------|
| Port          | Specifies the port the pluggable transceiver is installed in.        |
| Vendor Name   | Specifies the vendor's name for the installed pluggable transceiver. |
| Device Name   | Specifies the device name for the installed pluggable transceiver.   |
| Device Type   | Specifies the device type for the installed pluggable transceiver..  |
| Serial Number | Specifies the serial number for the installed pluggable transceiver. |

Table 4-7: Parameters in the output from the **show system pluggables detail** command: (cont.)

| Parameter              | Description                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Manufacturing Datecode | Specifies the manufacturing datecode for the installed pluggable transceiver. Checking the manufacturing datecode with the vendor may be useful when determining Laser Diode aging issues. For more information, see "How To Troubleshoot Fiber and Pluggable Issues" in the <a href="#">"Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide</a> .                              |
| SFP Laser Wavelength   | Specifies the laser wavelength of the installed pluggable transceiver.                                                                                                                                                                                                                                                                                                                                      |
| Single Mode Fiber      | Specifies the link length supported by the pluggable transceiver using single mode fiber.                                                                                                                                                                                                                                                                                                                   |
| OM1 (62.5um) Fiber     | Specifies the link length (in $\mu\text{m}$ - micron) supported by the pluggable transceiver using 62.5 micron multi-mode fiber.                                                                                                                                                                                                                                                                            |
| OM2 (50um) Fiber       | Specifies the link length (in $\mu\text{m}$ - micron) supported by the pluggable transceiver using 50 micron multi-mode fiber.                                                                                                                                                                                                                                                                              |
| Diagnostic Calibration | Specifies whether the pluggable transceiver supports DDM or DOM Internal or External Calibration:<br><b>Internal</b> is displayed if the pluggable transceiver supports DDM or DOM Internal Calibration.<br><b>External</b> is displayed if the pluggable transceiver supports DDM or DOM External Calibration.<br>- is displayed if SFP DDM Internal Calibration or External Calibration is not supported. |
| Power Monitoring       | Displays the received power measurement type, which can be either <b>OMA</b> (Optical Module Amplitude) or <b>Avg</b> (Average Power) measured in $\mu\text{W}$ .                                                                                                                                                                                                                                           |

**Related Commands**

- [show system environment](#)
- [show system pluggable](#)
- [show system pluggable diagnostics](#)



# show system pluggable diagnostics

**Overview** This command displays diagnostic information about SFP pluggable transceivers, which support Digital Diagnostic Monitoring (DDM).

Different types of pluggable transceivers are supported in different models of device. See your device's Datasheet for more information about the models of pluggables that your device supports.

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 system pluggable [*<port-list>*] diagnostics

| Parameter                | Description                                                                                                                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | The ports to display information about. The port list can be: <ul style="list-style-type: none"><li>• a switch port (e.g. port1.0.6)</li><li>• a continuous range of ports separated by a hyphen, e.g. port1.0.5-1.0.6</li><li>• a comma-separated list of ports and port ranges, e.g. port1.0.5, port1.0.6.</li></ul> |

**Mode** User Exec and Privileged Exec

**Usage** Modern optical SFP transceivers support Digital Diagnostics Monitoring (DDM) functions.

Diagnostic monitoring features allow you to monitor real-time parameters of the pluggable transceiver, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage. Additionally, RX LOS (Loss of Signal) is shown when the received optical level is below a preset threshold. Monitor these parameters to check on the health of all transceivers, selected transceivers or a specific transceiver installed in a device.

**Examples** To display detailed information about all pluggable transceivers installed on a standalone device, use the command:

```
awplus# show system pluggable diagnostics
```

**Output** Figure 4-23: Example output from the **show system pluggable diagnostics** command on a device

```
awplus#show system pluggable diagnostics
System Pluggable Information Diagnostics
```

| Port1.0.5         | Status  |       | Alarms |        |         | Warnings |        |
|-------------------|---------|-------|--------|--------|---------|----------|--------|
|                   | Reading | Alarm | Max    | Min    | Warning | Max      | Min    |
| Temp: (Degrees C) | 34.719  | -     | 110.00 | -45.00 | -       | 95.000   | -42.00 |
| Vcc: (Volts)      | 3.282   | -     | 3.600  | 3.000  | -       | 3.500    | 3.050  |
| Tx Bias: (mA)     | 23.024  | -     | 80.000 | 2.000  | -       | 70.000   | 3.000  |
| Tx Power: (mW)    | 0.357   | -     | 0.631  | 0.126  | -       | 0.501    | 0.159  |
| Rx Power: (mW)    | -       | Low   | 0.631  | 0.005  | Low     | 0.501    | 0.006  |
| Rx LOS:           | Rx Down |       |        |        |         |          |        |

Table 4-8: Parameters in the output from the **show system pluggables diagnostics** command

| Parameter        | Description                                                           |
|------------------|-----------------------------------------------------------------------|
| Temp (Degrees C) | Shows the temperature inside the transceiver.                         |
| Vcc (Volts)      | Shows voltage supplied to the transceiver.                            |
| Tx Bias (mA)     | Shows current to the Laser Diode in the transceiver.                  |
| Tx Power (mW)    | Shows the amount of light transmitted from the transceiver.           |
| Rx Power (mW)    | Shows the amount of light received in the transceiver.                |
| Rx LOS           | Shows when the received optical level falls below a preset threshold. |

**Related Commands**

- [show system environment](#)
- [show system pluggable](#)
- [show system pluggable detail](#)

# show system serialnumber

**Overview** This command shows the serial number information for 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 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 4-24: Example output from the **show system serial number** 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. You can optionally limit the command output to display only information for a given protocol or feature.

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.

**Syntax** show tech-support  
{all|[atmf|dhcpsn|epsr|igmp|ip|ipv6|mld|pim|stp|system|tacacs+]  
|[outfile <filename>]}

| Parameter  | Description                                                                                                     |
|------------|-----------------------------------------------------------------------------------------------------------------|
| all        | Display full information                                                                                        |
| atmf       | Display ATMF- specific information                                                                              |
| dhcpsn     | Display DHCP Snooping specific information                                                                      |
| epsr       | Display EPSR specific information                                                                               |
| igmp       | Display IGMP specific information                                                                               |
| ip         | Display IP specific information                                                                                 |
| ipv6       | Display IPv6 specific information                                                                               |
| mld        | Display MLD specific information                                                                                |
| outfile    | Output file name                                                                                                |
| pim        | Display PIM related information                                                                                 |
| stp        | Display STP specific information                                                                                |
| system     | Display general system information                                                                              |
| tacacs+    | Display TACACS+ information                                                                                     |
|            | Output modifier                                                                                                 |
| >          | Output redirection                                                                                              |
| >>         | Output redirection (append)                                                                                     |
| <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-support20080109.txt.gz', so the last saved file is retained.

**Usage** This command is useful for collecting a large amount of information about all protocols or specific protocols on your device 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.

**Mode** Privileged Exec

**Examples** show tech-support  
awplus# show tech-support

## speed (asyn)

**Overview** This command changes the console speed from the device. Note that a change in console speed is applied for subsequent console sessions. Exit the current session to enable the console speed change using the [clear line console](#) command.

**CAUTION:** The bootloader on an IE200-6 Series switch always runs at 9600 Baud. If you change the baud rate, you will be unable to access to the bootloader.

**Syntax** speed <console-speed-in-bps>

| Parameter              | Description                                       |
|------------------------|---------------------------------------------------|
| <console-speed-in-bps> | Console speed Baud rate in bps (bits per second). |
| 1200                   | 1200 Baud                                         |
| 2400                   | 2400 Baud                                         |
| 9600                   | 9600 Baud                                         |
| 19200                  | 19200 Baud                                        |
| 38400                  | 38400 Baud                                        |
| 57600                  | 57600 Baud                                        |
| 115200                 | 115200 Baud                                       |

**Default** The default console speed baud rate is 9600 bps.

**Mode** Line Configuration

**Usage** This command is used to change the console (asyn) port speed. Set the console speed to match the transmission rate of the device connected to the console (asyn) port on your device.

**Example** To set the terminal console (asyn0) port speed from the device to 57600 bps, then exit the session, use the commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# speed 57600
awplus(config-line)# exit
awplus(config)# exit
awplus# exit
```

Then log in again to enable the change:

```
awplus login:
Password:
awplus>
```

**Related  
Commands**

- clear line console
- line
- show running-config
- show startup-config
- speed

# system territory (deprecated)

**Overview** This command has been deprecated in version 5.4.4-0.1. It now has no effect.



# 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** to stop displaying debugging output on the terminal, or use the timeout option to stop displaying debugging output on the terminal after a set time.

**Syntax** terminal monitor [<1-60>]  
terminal no 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 specify timeout of debugging output after 60 seconds, enter the command:

```
awplus# terminal monitor 60
```

To stop displaying debugging output on the terminal, use the command:

```
awplus# terminal no monitor
```

**Related  
Commands** All debug commands

# undebug all

**Overview** This command applies the functionality of the [no debug all](#) command.

# 5

# Logging Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure logging.

- Command List**
- “clear exception log” on page 229
  - “clear log” on page 230
  - “clear log buffered” on page 231
  - “clear log permanent” on page 232
  - “default log buffered” on page 233
  - “default log console” on page 234
  - “default log email” on page 235
  - “default log host” on page 236
  - “default log monitor” on page 237
  - “default log permanent” on page 238
  - “log buffered” on page 239
  - “log buffered (filter)” on page 240
  - “log buffered size” on page 243
  - “log console” on page 244
  - “log console (filter)” on page 245
  - “log email” on page 248
  - “log email (filter)” on page 249
  - “log email time” on page 252
  - “log host” on page 254
  - “log host (filter)” on page 255

- [“log host time”](#) on page 258
- [“log monitor \(filter\)”](#) on page 260
- [“log permanent”](#) on page 263
- [“log permanent \(filter\)”](#) on page 264
- [“log permanent size”](#) on page 267
- [“log-rate-limit nsm”](#) on page 268
- [“show counter log”](#) on page 270
- [“show exception log”](#) on page 271
- [“show log”](#) on page 272
- [“show log config”](#) on page 275
- [“show log permanent”](#) on page 278
- [“show running-config log”](#) on page 279

# clear exception log

**Overview** This command resets the contents of the exception log, but does not remove the associated core files.

**NOTE:** *When this command is used within a stacked environment, it will remove the contents of the exception logs in all stack members.*

**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.

**NOTE:** When this command is used within a stacked environment, it will remove the contents of the buffered and permanent logs in all stack members.

**Syntax** clear log

**Mode** Privileged Exec

**Example** To delete the contents of the buffered and permanent log use the command:

```
awplus# clear log
```

**Validation  
Commands** show log

**Related  
Commands** clear log buffered  
clear log permanent

# 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
```

**Validation  
Commands** show log

**Related  
Commands** clear log  
clear log permanent

# clear log permanent

**Overview** This command removes the contents of the permanent log.

**NOTE:** *When this command is used within a stacked environment, it will remove the contents of the buffered logs in all stack members.*

The permanent log is stored in NVS. On IE200-6 Series switches, files in NVS persist over a device restart but do not persist over a power cycle.

**Syntax** `clear log permanent`

**Mode** Privileged Exec

**Example** To delete the contents of the permanent log use the following commands:

```
awplus# clear log permanent
```

**Validation  
Commands** `show log`

**Related  
Commands** `clear log`  
`clear log buffered`



# 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
```

**Validation  
Commands** `show log config`

**Related  
Commands** `log buffered`  
`log buffered size`

# 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
```

**Validation  
Commands** `show log config`

**Related  
Commands** `log console`  
`log console (filter)`

# 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>&lt;email-address&gt;</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** [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>&lt;ip-addr&gt;</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
```

**Validation  
Commands** [show log config](#)

**Related  
Commands** [log email](#)

# 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 \(filter\)](#)  
[show log config](#)

# 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.

The permanent log is stored in NVS. On IE200-6 Series switches, files in NVS persist over a device restart but do not persist over a power cycle.

**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** [log permanent](#)  
[log permanent size](#)  
[show log config](#)

# 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
```

**Validation  
Commands** show log config

**Related  
Commands** default log buffered  
log buffered (filter)  
log buffered size

# 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.                                                                                        |



| Parameter                                                 | Description                                                                                                                                                                                      |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;program-name&gt;facility&lt;facility&gt;</code> | The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output: |
|                                                           | rsvp Resource Reservation Protocol (RSVP)                                                                                                                                                        |
|                                                           | 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)                                                                                                                                                   |
|                                                           | rmon Remote Monitoring                                                                                                                                                                           |
|                                                           | loopprot Loop Protection                                                                                                                                                                         |
|                                                           | poe Power-inline (Power over Ethernet)                                                                                                                                                           |
|                                                           | dhcpcsn DHCP snooping (DHCP SN)                                                                                                                                                                  |
|                                                           | Filter messages to the buffered log by syslog 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.                                                                                                                                                |
| <code>&lt;text-string&gt;</code>                          | 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 generated by EPSR that have a severity of **notices** or higher to the buffered log use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# log buffered level notices program epsr
```

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 generated by EPSR that have a severity of **notices** or higher to the buffered log use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no log buffered level notices program epsr
```

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
```

**Validation  
Commands** [show log config](#)

**Related  
Commands** [default log buffered](#)  
[log buffered](#)  
[log buffered size](#)

# 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.

**Syntax** log buffered size <50-250>

| Parameter  | Description                      |
|------------|----------------------------------|
| <50 - 250> | Size of the RAM log in kilobytes |

**Mode** Global Configuration

**Example** To allow the buffered log to use up to 100 kB of RAM use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered size 100
```

**Validation  
Commands** show log config

**Related  
Commands** default log buffered  
log buffered

# 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 devices 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
```

**Validation  
Commands** show log config

**Related  
Commands** log console (filter)

# 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.                                                                                                            |

| Parameter                                                 | Description                                                                                                                                                                                      |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;program-name&gt;facility&lt;facility&gt;</code> | The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output: |
|                                                           | rsvp Resource Reservation Protocol (RSVP)                                                                                                                                                        |
|                                                           | 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)                                                                                                                                                   |
|                                                           | rmon Remote Monitoring                                                                                                                                                                           |
|                                                           | loopprot Loop Protection                                                                                                                                                                         |
|                                                           | poe Power-inline (Power over Ethernet)                                                                                                                                                           |
|                                                           | dhcpsn DHCP snooping (DHCP SN)                                                                                                                                                                   |
|                                                           | Filter messages by syslog 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.                                                                                                                                                |
| <code>&lt;text-string&gt;</code>                          | 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 `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 generated by MSTP that have a severity of `info` or higher to console instances where the `log console` command has been given, remove the default filter that includes everything use the following commands:

```
awplus# configure terminal
awplus(config)# log console level info program mstp
```

and then use the command:

```
awplus(config)# log console level info program mstp
```

To create a filter to send all messages containing the text “Bridging initialization” to console instances where the `log console` command has been given use the following commands:

```
awplus# configure terminal
awplus(config)# log console msgtext "Bridging initialization"
```

To remove a filter that sends all messages generated by EPSR that have a severity of notices or higher to consoles use the following commands:

```
awplus# configure terminal
awplus(config)# no log console level notices program epsr
```

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
```

**Validation  
Commands** [show log config](#)

**Related  
Commands** [log console](#)

# 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>&lt;email-address&gt;</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
```

**Validation  
Commands** `show log config`

**Related  
Commands** `default log email`  
`log email`



# 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                                                                                                                                                                       |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <email-address> | The email address to send logging messages to                                                                                                                                     |
| 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.                                                                                                            |

| Parameter                                                 | Description                                                                                                                                                                                      |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;program-name&gt;facility&lt;facility&gt;</code> | The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output: |
|                                                           | rsvp Resource Reservation Protocol (RSVP)                                                                                                                                                        |
|                                                           | 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)                                                                                                                                                   |
|                                                           | rmon Remote Monitoring                                                                                                                                                                           |
|                                                           | loopprot Loop Protection                                                                                                                                                                         |
|                                                           | poe Power-inline (Power over Ethernet)                                                                                                                                                           |
|                                                           | dhcpcsn DHCP snooping (DHPCSN)                                                                                                                                                                   |
|                                                           | Filter messages by syslog 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.                                                                                                                                                |
| <code>&lt;text-string&gt;</code>                          | 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 generated by EPSR that have a severity of notices or higher to the email address `admin@homebase.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@homebase.com level notices
program epsr
```

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 all messages generated by EPSR that have a severity of notices or higher to the email address `admin@homebase.com` use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@homebase.com level notices
program epsr
```

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](#)  
[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 <b>plus</b> or <b>minus</b> 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 <b>plus</b> or <b>minus</b> 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** 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
```

**Validation  
Commands** `show log config`

**Related  
Commands** `default log buffered`

# 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.

**Syntax** log host <ip-addr>  
no log host <ip-addr>

| Parameter | Description                                                               |
|-----------|---------------------------------------------------------------------------|
| <ip-addr> | The IP address of a remote syslog server in dotted decimal format A.B.C.D |

**Mode** Global Configuration

**Examples** To configure the device to send log messages to a remote syslog server with IP address 10.32.16.99 use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.99
```

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
```

**Validation Commands** show log config

**Related Commands** default log host

# 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: |
| 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.                                                                                                            |

| Parameter                                                 | Description                                                                                                                                                                                      |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;program-name&gt;facility&lt;facility&gt;</code> | The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output: |
|                                                           | rsvp Resource Reservation Protocol (RSVP)                                                                                                                                                        |
|                                                           | 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)                                                                                                                                                   |
|                                                           | rmon Remote Monitoring                                                                                                                                                                           |
|                                                           | loopprot Loop Protection                                                                                                                                                                         |
|                                                           | poe Power-inline (Power over Ethernet)                                                                                                                                                           |
|                                                           | dhcpcsn DHCP snooping (DHPCSN)                                                                                                                                                                   |
|                                                           | Filter messages by syslog 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.                                                                                                                                                |
| <code>&lt;text-string&gt;</code>                          | 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 generated by EPSR that have a severity of notices or higher 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 level notices program epsr
```

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 generated by EPSR that have a severity of notices or higher 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 level notices program
epsr
```

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](#)  
[show log config](#)

# 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 <email-address> time {local|local-offset|utc-offset {plus|minus} <0-24>}`

| Parameter                          | Description                                                                                                                                                                                                    |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;email-address&gt;</code> | The email address to send log messages to                                                                                                                                                                      |
| <code>time</code>                  | Specify the time difference between the email recipient and the device you are configuring.                                                                                                                    |
| <code>local</code>                 | The device is in the same time zone as the email recipient                                                                                                                                                     |
| <code>local-offset</code>          | The device is in a different time zone to the email recipient. Use the <b>plus</b> or <b>minus</b> keywords and specify the difference (offset) from local time of the device to the email recipient in hours. |
| <code>utc-offset</code>            | The device is in a different time zone to the email recipient. Use the <b>plus</b> or <b>minus</b> keywords and specify the difference (offset) from UTC time of the device to the email recipient in hours.   |
| <code>plus</code>                  | Negative offset (difference) from the device to the syslog server.                                                                                                                                             |
| <code>minus</code>                 | Positive offset (difference) from the device to the syslog server.                                                                                                                                             |
| <code>&lt;0-24&gt;</code>          | World Time zone offset in hours                                                                                                                                                                                |

**Default** The default is **local** time.

**Mode** Global Configuration

**Usage** 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
```

**Validation  
Commands**    [show log config](#)

**Related  
Commands**    [default log buffered](#)

# 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: |
| 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.                                                                                                            |

| Parameter                                                 | Description                                                                                                                                                                                      |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;program-name&gt;facility&lt;facility&gt;</code> | The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output: |
|                                                           | rsvp Resource Reservation Protocol (RSVP)                                                                                                                                                        |
|                                                           | 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)                                                                                                                                                   |
|                                                           | rmon Remote Monitoring                                                                                                                                                                           |
|                                                           | loopprot Loop Protection                                                                                                                                                                         |
|                                                           | poe Power-inline (Power over Ethernet)                                                                                                                                                           |
|                                                           | dhcpcsn DHCP snooping (DHCP SN)                                                                                                                                                                  |
|                                                           | Filter messages by syslog 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.                                                                                                                                                |
| <code>&lt;text-string&gt;</code>                          | 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 generated by MSTP that 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 mstp
```

To remove a filter that sends all messages generated by EPSR that have a severity of notices or higher to the terminal use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no log monitor level notices program epsr
```

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
```

**Validation  
Commands** [show log config](#)

**Related  
Commands** [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.

On IE200-6 Series switches, files in NVS persist over a device restart but do not persist over a power cycle.

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
```

**Validation  
Commands** show log config

**Related  
Commands** default log permanent  
log permanent (filter)  
log permanent size  
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 permanent log is stored in NVS. On IE200-6 Series switches, files in NVS persist over a device restart but do not persist over a power cycle.

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.                                                                                                            |



| Parameter                                                 | Description                                                                                                                                                                                      |
|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;program-name&gt;facility&lt;facility&gt;</code> | The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output: |
|                                                           | rsvp Resource Reservation Protocol (RSVP)                                                                                                                                                        |
|                                                           | 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)                                                                                                                                                   |
|                                                           | rmon Remote Monitoring                                                                                                                                                                           |
|                                                           | loopprot Loop Protection                                                                                                                                                                         |
|                                                           | poe Power-inline (Power over Ethernet)                                                                                                                                                           |
|                                                           | dhcpsn DHCP snooping (DHCP SN)                                                                                                                                                                   |
|                                                           | Filter messages by syslog 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.                                                                                                                                                |
| <code>&lt;text-string&gt;</code>                          | 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 generated by EPSR that have a severity of notices or higher to the permanent log use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# log permanent level notices program epsr
```

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
```

**Validation  
Commands** [show log config](#)

**Related  
Commands** [default log permanent](#)  
[log permanent](#)  
[log permanent size](#)  
[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.

The permanent log is stored in NVS. On IE200-6 Series switches, files in NVS persist over a device restart but do not persist over a power cycle.

**Syntax** log permanent size <50-250>

| Parameter | Description                            |
|-----------|----------------------------------------|
| <50-250>  | Size of the permanent log in kilobytes |

**Mode** Global Configuration

**Example** To allow the permanent log to use up to 100 kB of NVS use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent size 100
```

**Validation  
Commands** [show log config](#)

**Related  
Commands** [default log permanent](#)  
[log permanent](#)

# log-rate-limit nsm

**Overview** This command limits the number of log messages generated by the device for a given interval.

Use the **no** variant of this command to revert to the default number of log messages generated by the device of 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                                                                                                                                                           |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;message-limit&gt;</i> | <i>&lt;1-65535&gt;</i><br>The number of log messages generated by the device.                                                                                         |
| <i>&lt;time-interval&gt;</i> | <i>&lt;0-65535&gt;</i><br>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** Previously, if the device received a continuous stream of IGMP packets with errors, such as when a packet storm occurs because of a network loop, then the device generates a lot of log messages using more and more memory, which may ultimately cause the device to shutdown. This log rate limiting feature constrains the rate that log messages are generated by the device.

Note that if within the given time interval, the number of log messages exceeds the limit, then any excess log messages are discarded. At the end of the time interval, a single log message is generated indicating that log messages were discarded due to the log rate limit being exceeded.

Thus if the expectation is that there will be a lot of discarded log messages due to log rate limiting, then it is advisable to set the time interval to no less than 100, which means that there would only be one log message, indicating log excessive log messages have been discarded.

**Examples** To limit the device to generate up to 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 the default setting, to generate up to 200 log messages per second, use the following commands:

```
awplus# configure terminal
awplus(config)# no log-rate-limit nsm
```

# 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 5-1: 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 5-1: 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.

**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 5-2: Example output from the **show exception log** command on a device

```
awplus#show exception log
<date> <time> <facility>.<severity> <program[<pid>]>: <message>

2014 Jan 08 08:05:59 local7.debug awplus corehandler : Process hsl (PID:741) sig
nal 11, core dumped to /flash/hsl-IE200-proj1747_ie200-20131225-1-1-1262937958-7
41.tgz
2014 Jan 08 08:17:43 local7.debug awplus corehandler : Process hsl (PID:745) sig
nal 11, core dumped to /flash/hsl-IE200-proj1747_IE200-20131225-1-1-1262938662-7
45.tgz

```

**Output** Figure 5-3: Example output from the **show exception log** command on a switch 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 “Controlling “show” Command Output” in 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** 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.

**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 5-4: Example output from the **show log** command

```
awplus#show log

<date> <time> <facility>.<severity> <program[<pid>]>: <message>

2011 Aug 29 07:55:22 kern.notice awplus kernel: Linux version 2.6.32.12-at1 (maker@awpmaker03-dl) (gcc version 4.3.3 (Gentoo 4.3.3-r3 p1.2, pie-10.1.5)) #1 Wed Dec 8 11:53:40 NZDT 2010
2011 Aug 29 07:55:22 kern.warning awplus kernel: No pci config register base in dev tree, using default
2011 Aug 29 07:55:23 kern.notice awplus kernel: Kernel command line: console=ttyS0,9600 releasefile=IE200-5.4.5I-01.rel ramdisk=14688
bootversion=1.1.0-rc12 loglevel=1
extraflash=00000000
2011 Aug 29 07:55:25 kern.notice awplus kernel: RAMDISK: squashfs filesystem found at block 0
2011 Aug 29 07:55:28 kern.warning awplus kernel: ipifwd: module license 'Proprietary' taints kernel.

.
.
.
```

Figure 5-5: Example output from the **show log tail** command

```
awplus#show log tail

<date> <time> <facility>.<severity> <program[<pid>]>: <message>

2006 Nov 10 13:30:01 cron.notice crond[116]: USER manager pid 469 cmd logrotate /
etc/logrotate.conf

2006 Nov 10 13:30:01 cron.notice crond[116]: USER manager pid 471 cmd nbqueue --
wipe

2006 Nov 10 13:35:01 cron.notice crond[116]: USER manager pid 472 cmd nbqueue --
wipe

2006 Nov 10 13:40:01 cron.notice crond[116]: USER manager pid 477 cmd nbqueue --
wipe

2006 Nov 10 13:44:36 syslog.notice syslog-ng[67]: Log statistics;
processed=\'center(queued)=70\' , processed=\'2006 Nov 10 13:45:01 cron.notice
crond[116]: USER manager pid 478 cmd logrotate /etc/logrotate.conf

2006 Nov 10 13:45:01 cron.notice crond[116]: USER manager pid 480 cmd nbqueue --
wipe

2006 Nov 10 13:49:32 syslog.notice syslog-ng[67]: SIGHUP received, reloading
configuration;

2006 Nov 10 13:50:01 cron.notice crond[116]: USER manager pid 482 cmd nbqueue --
wipe

2006 Nov 10 13:55:01 cron.notice crond[116]: USER manager pid 483 cmd nbqueue --
wipe

.
.
.
```

**Related  
Commands**    [show log config](#)  
              [show log permanent](#)

# show log config

**Overview** This command displays information about the logging system. This includes the configuration of the various log destinations, buffered, permanent, syslog servers (hosts) and email addresses. This also displays the latest status information for each of these destinations.

**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 5-6: Example output from the **show log config** command

```
Buffered log:
Status enabled
Maximum size ... 100kb
Filters:
*1 Level notices
 Program any
 Facility any
 Message text . any
 2 Level informational
 Program mstp
 Facility daemon
 Message text . any
Statistics 1327 messages received, 821 accepted by filter (2006 Dec 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 (2006 Dec 11
10:36:16)
Host 10.32.16.21:
Time offset +2:00
Offset type UTC
Filters:
 1 Level critical
 Program any
 Facility any
 Message text . any
Statistics 1327 messages received, 1 accepted by filter (2006 Dec 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 (2006 Dec 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.

The permanent log is stored in NVS. On IE200-6 Series switches, files in NVS persist over a device restart but do not persist over a power cycle.

**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. |

**Default** 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 select 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 5-7: Example output from the **show log permanent** command

```
awplus#show log permanent

<date> <time> <facility>.<severity> <program[<pid>]>: <message>

2014 Jun 10 09:30:09 syslog.notice syslog-ng[67]: syslog-ng starting up;
version='2.0rc3'

2014 Jun 10 09:30:09 auth.warning portmap[106]: user rpc not found, reverting to
user bin

2014 Jun 10 09:30:09 cron.notice crond[116]: crond 2.3.2 dillon, started, log
level 8

2014 Jun 10 09:30:14 daemon.err snmpd[181]: /flash/.configs/snmpd.conf: line 20:
Error: bad SUBTREE object
2014 Jun 10 09:30:14 user.info HSL[192]: HSL: INFO: Registering port port1.0.1
```

**Related  
Commands** [show log](#)

# 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](#)

# 6

# Scripting Commands

## Introduction

**Overview** This chapter provides commands used for command scripts.

- Command List**
- [“activate”](#) on page 281
  - [“echo”](#) on page 282
  - [“wait”](#) on page 283



# activate

**Overview** This command activates a script file.

**Syntax** activate [background] <script>

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                   |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| background | 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. |
| <script>   | 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 <b>.scp</b> or a <b>.sh</b> filename extension for a valid script text file, as described below in the usage section for this command.                                  |

**Mode** Privileged Exec

**Usage** 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        |
|-----------|--------------------|
| <line>    | 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                                   |
|-----------|-----------------------------------------------|
| <delay>   | <1 - 65335> Specify the time delay in seconds |

**Default** No wait delay is specified by default to pause script execution.

**Mode** Privileged Exec (when executed from a script not directly from the command line)

**Usage** 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 \(Privileged Exec mode\)](#) command since the **wait** command is only executed in the Privileged Exec mode. 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.

**Example** See an example **.scp** script file extract below that will show port counters for interface port1.0.1 over a 10 second interval:

```
enable

show interface port1.0.1

wait 10

show interface port1.0.1
```

**Related Commands**

- [activate](#)
- [echo](#)
- [enable \(Privileged Exec mode\)](#)

# 7

# Interface Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure and display interfaces.

- Command List**
- “[description \(interface\)](#)” on page 285
  - “[interface \(to configure\)](#)” on page 286
  - “[mru jumbo](#)” on page 288
  - “[mtu](#)” on page 289
  - “[show interface](#)” on page 291
  - “[show interface brief](#)” on page 294
  - “[show interface status](#)” on page 295
  - “[shutdown](#)” on page 297

# description (interface)

**Overview** Use this command to add a description to a specific port or interface.

**Syntax** `description <description>`

| Parameter                        | Description                             |
|----------------------------------|-----------------------------------------|
| <code>&lt;description&gt;</code> | Text describing the specific interface. |

**Mode** Interface Configuration

**Example** The following example uses this command to describe the device that a switch port is connected to.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# description Boardroom PC
```

# interface (to configure)

**Overview** Use this command to select one or more interfaces to configure.

**Syntax** `interface <interface-list>`  
`interface lo`

| Parameter                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;interface-list&gt;</code> | The interfaces or ports to configure.<br>An interface-list can be: <ul style="list-style-type: none"><li>• an interface such as a VLAN (e.g. <code>vlan2</code>), a switch port (e.g. <code>port1.0.6</code>), a static channel group (e.g. <code>sa2</code>) or a dynamic (LACP) channel group (e.g. <code>po2</code>)</li><li>•</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. <code>vlan2-8</code>, or <code>port1.0.1-1.0.6</code>, or <code>sa1-2</code>, or <code>po1-2</code></li><li>• a comma-separated list of the above; e.g. <code>port1.0.1, port1.0.4-1.0.6</code>. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |
| <code>lo</code>                     | The local loopback interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Usage** 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

**Example** The following example shows how to enter Interface mode to configure `vlan1`. Note how the prompt changes.

```
awplus# configure terminal
awplus(config)# interface vlan1
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)#
```

**Related  
Commands**

[ip address](#)  
[show interface](#)  
[show interface brief](#)

# mru jumbo

**Overview** Use this command to enable the device to forward jumbo frames. For more information, see the [Switching Feature Overview and Configuration Guide](#).

When jumbo frame support is enabled, the maximum size of packets that the device can forward is 9710 bytes of payload.

Use the no variant of this command to remove jumbo frame support, and restore the default MRU size (1500 bytes) for switch ports.

**NOTE:**

*The figure of 1500 or 9710 bytes specifies the payload only. For an IEEE 802.1q frame, provision is made (internally) for the following additional components:*

- Source and Destination addresses
- EtherType field
- Priority and VLAN tag fields
- FCS

These additional components increase the frame size internally (to 1522 bytes in the default case).

**Syntax** mru jumbo  
no mru

**Default** By default, jumbo frame support is not enabled.

**Mode** Interface Configuration for switch ports.

**Usage** Note that [show interface](#) output will only show MRU size for switch ports.

We recommend limiting the number of ports with jumbo frames support enabled to two.

**Examples** To enable the device to forward jumbo frames on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# mru jumbo
```

To remove the jumbo frame support, and therefore restore the MRU size of 1500 bytes on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no mru
```

**Related Commands** [show interface](#)



# mtu

**Overview** Use this command to set the Maximum Transmission Unit (MTU) size for VLANs, where MTU is the maximum packet size that VLANs 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 for VLANs, and restore the default MTU size (1500 bytes) for VLANs.

**Syntax** `mtu <mtu-size>`  
`no mtu`

| Parameter                     | Description                                                                                                                                                      |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;mtu-size&gt;</code> | <code>&lt;68-1582&gt;</code><br>Specifies the Maximum Transmission Unit (MTU) size in bytes, where 1500 bytes is the default Ethernet MTU size for an interface. |

**Default** The default MTU size is 1500 bytes for VLAN interfaces.

**Mode** Interface Configuration for VLAN interfaces.

**Usage** If a device receives an IPv4 packet for Layer 3 switching to another VLAN 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 VLAN interface, an ICMP ' **packet too big**' (ICMP type 2 code 0) message is sent to the source.

Note that [show interface](#) output will only show MTU size for VLAN interfaces.

**Examples** To configure an MTU size of 1500 bytes on interface `v lan2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# mtu 1500
```

To configure an MTU size of 1500 bytes on interfaces `v lan2` to `v lan4`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# mtu 1500
```

To restore the MTU size to the default MTU size of 1500 bytes on `v lan2`, use the commands

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no mtu
```

To restore the MTU size to the default MTU size of 1500 bytes on v l a n 2 and v l a n 4, use the commands

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no mtu
```

**Related  
Commands**   [show interface](#)

# show interface

**Overview** Use this command to display interface configuration and status.

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 interface [*<interface-list>*]  
show interface lo

| Parameter                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;interface-list&gt;</i> | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• an interface such as a VLAN (e.g. v lan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>•</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v lan2-8, or port1.0.1-1.0.6, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |
| lo                            | The local loopback interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

**Mode** User Exec and Privileged Exec

**Usage** Note that the output displayed with this command will show MTU (Maximum Transmission Unit) size for VLAN interfaces, and MRU (Maximum Received Unit) size for switch ports.

**Example** To display configuration and status information for all interfaces, use the command:

```
awplus# show interface
```

Figure 7-1: Example output from the **show interface** command

```
awplus#show interface
Interface port1.0.1
 Scope: both
 Link is DOWN, administrative state is UP
 Thrash-limiting
 Status Not Detected, Action learn-disable, Timeout 1(s)
 Hardware is Ethernet, address is 000c.2503.9a74
 index 5001 metric 1 mru 1518
 configured duplex auto, configured speed auto, configured polarity auto
 <UP,BROADCAST,MULTICAST>
 SNMP link-status traps: 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 00:12:18
Interface port1.0.2
 Scope: both
 Link is UP, administrative state is UP
 Thrash-limiting
 Status Not Detected, Action learn-disable, Timeout 1(s)
 Hardware is Ethernet, address is 000c.2503.9a74
 index 5002 metric 1 mru 1518
 current duplex full, current speed 100, current polarity mdi
 configured duplex auto, configured speed auto, configured polarity auto
 <UP,BROADCAST,RUNNING,MULTICAST>
 SNMP link-status traps: Disabled
 input packets 4566, bytes 530517, dropped 0, multicast packets 753
 output packets 0, bytes 0, multicast packets 0 broadcast packets 0
 Time since last state change: 0 days 00:10:31
...
Interface lo
 Scope: both
 Link is UP, administrative state is UP
 Hardware is Loopback
 index 1 metric 1
 <UP,LOOPBACK,RUNNING>
 SNMP link-status traps: 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 00:12:18
Interface vlan1
 Scope: both
 Link is DOWN, administrative state is DOWN
 Hardware is VLAN, address is 000c.2503.9a74
 index 301 metric 1 mtu 1500
 arp ageing timeout 300
 <BROADCAST,MULTICAST>
 SNMP link-status traps: Disabled
 Bandwidth 1g
 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 00:12:18
```

To display configuration and status information for interface **lo**, use the command:

```
awplus# show interface lo
```

Figure 7-2: Example output from the **show interface lo** command

```
awplus#show interface lo
Interface lo
 Scope: both
 Link is UP, administrative state is UP
 Hardware is Loopback
 index 1 metric 1
 <UP,LOOPBACK,RUNNING>
 SNMP link-status traps: 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: 69 days 01:28:47
```

To display configuration and status information for interfaces `vlan1` and `vlan2`, use the command:

```
awplus# show interface vlan1,vlan2
```

Figure 7-3: Example output from the **show interface vlan1,vlan2** command

```
awplus#show interface vlan1,vlan2
Interface vlan1
 Scope: both
 Link is UP, administrative state is UP
 Hardware is VLAN, address is 0015.77e9.5c50
 IPv4 address 192.168.1.1/24 broadcast 192.168.1.255
 index 201 metric 1 mtu 1500
 arp ageing timeout 300
 <UP,BROADCAST,RUNNING,MULTICAST>
 SNMP link-status traps: Disabled
 Bandwidth 1g
 input packets 295606, bytes 56993106, dropped 5, multicast packets 156
 output packets 299172, bytes 67379392, multicast packets 0 broadcast packets 0
 Time since last state change: 0 days 14:22:39

Interface vlan2
 Scope: both
 Link is DOWN, administrative state is UP
 Hardware is VLAN, address is 0015.77e9.5c50
 IPv4 address 192.168.2.1/24 broadcast 192.168.2.255
 Description: ip_phone_vlan
 index 202 metric 1 mtu 1500
 arp ageing timeout 300
 <UP,BROADCAST,MULTICAST>
 SNMP link-status traps: Disabled
 Bandwidth 1g
 input packets 0, bytes 0, dropped 0, multicast packets 0
 output packets 90, bytes 4244, multicast packets 0 broadcast packets 0
 Time since last state change: 0 days 14:22:39
```

**Related Commands**

- [mru jumbo](#)
- [mtu](#)
- [show interface brief](#)

# 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show interface brief

**Mode** User Exec and Privileged Exec

**Output** Figure 7-4: Example output from the **show interface brief** command

```
awplus# show interface brief
Interface Status Protocol
port1.0.1 admin up down
port1.0.2 admin up running
port1.0.3 admin up down
port1.0.4 admin up down
port1.0.5 admin up down
port1.0.6 admin up down
lo admin up running
vlan1 admin down down
```

Table 7-1: Parameters in the output of the **show interface brief** command

| Parameter | Description                                                                               |
|-----------|-------------------------------------------------------------------------------------------|
| Interface | The name or type of interface.                                                            |
| Status    | The administrative state. This can be either <b>admin up</b> or <b>admin down</b> .       |
| Protocol  | The link state. This can be either <b>down</b> , <b>running</b> , or <b>provisioned</b> . |

**Related Commands** [show interface](#)  
[show interface memory](#)

# 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                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;port-list&gt;</code> | <p>The ports to display information about. The port list can be:</p> <ul style="list-style-type: none"> <li>a switch port (e.g. port1.0.6) a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li> <li>a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.6, or sa1-2, or po1-2</li> <li>a comma-separated list of ports and port ranges, e.g. port1.0.1, port1.0.4-1.0.6. Do not mix switch ports, static channel groups, and dynamic (LACP) channel groups in the same list</li> </ul> |

**Examples** To display the status of ports 1.0.1 to 1.0.5, use the commands:

```
awplus# show interface port1.0.1-1.0.4 status
```

Table 7-2: Example output from the **show interface <port-list> status** command

```
awplus#show interface port1.0.1 -1.0.5 status
```

| Port      | Name | Status     | Vlan | Duplex | Speed | Type       |
|-----------|------|------------|------|--------|-------|------------|
| port1.0.1 |      | notconnect | 1    | auto   | auto  | 1000BASE-T |
| port1.0.2 |      | notconnect | 1    | auto   | auto  | 1000BASE-T |
| port1.0.3 |      | notconnect | 1    | auto   | auto  | 1000BASE-T |
| port1.0.4 |      | notconnect | 1    | auto   | auto  | 1000BASE-T |

To display the status of all ports, use the commands:

```
awplus# show interface status
```

Table 7-3: Example output from the **show interface status** command

```
awplus#show interface status
```

| Port      | Name | Status     | Vlan | Duplex | Speed | Type       |
|-----------|------|------------|------|--------|-------|------------|
| port1.0.1 |      | notconnect | 1    | auto   | auto  | 1000BASE-T |
| port1.0.2 |      | connected  | 1    | a-full | a-100 | 1000BASE-T |
| port1.0.3 |      | notconnect | 1    | auto   | auto  | 1000BASE-T |
| port1.0.4 |      | notconnect | 1    | auto   | auto  | 1000BASE-T |
| port1.0.5 |      | notconnect | 1    | auto   | auto  | BASE-BX10  |
| port1.0.6 |      | notconnect | 1    | auto   | auto  | BASE-BX10  |

Table 7-4: 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: <ul style="list-style-type: none"> <li>disabled: the interface is administratively down.</li> <li>connect: the interface is operationally up.</li> <li>notconnect: the interface is operationally down.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Vlan      | VLAN type or VLAN IDs associated with the port: <ul style="list-style-type: none"> <li>When the VLAN mode is trunk, it displays <b>trunk</b> (it does not display the VLAN IDs).</li> <li>When the VLAN mode is access, it displays the VLAN ID.</li> <li>When the VLAN mode is private promiscuous, it displays the primary VLAN ID if it has one, and <b>promiscuous</b> if it does not have a VLAN ID.</li> <li>When the VLAN mode is private host, it displays the primary and secondary VLAN IDs.</li> <li>When the port is an Eth port, it displays <b>none</b>: there is no VLAN associated with it.</li> <li>When the VLAN is dynamically assigned, it displays the current dynamically assigned VLAN ID (not the access VLAN ID), or <b>dynamic</b> if it has multiple VLANs dynamically assigned.</li> </ul> |
| Duplex    | The actual duplex mode of the interface, preceded by <b>a-</b> 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 <b>a-</b> 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. For SFP bays, it displays <b>Unknown</b> if it does not recognize the type of SFP installed, or <b>Not present</b> if an SFP is not installed or is faulty.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Related Commands** [show interface](#)  
[show interface memory](#)



# 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 therefore to bring the link back up again.

**Syntax** shutdown  
no shutdown

**Mode** Interface Configuration

**Example** The following example shows the use of the **shutdown** command to shut down port1.0.2.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# shutdown
```

The following example shows the use of the **no shutdown** command to bring up port1.0.2.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no shutdown
```

The following example shows the use of the **shutdown** command to shut down vlan2.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# shutdown
```

The following example shows the use of the **no shutdown** command to bring up vlan2.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no shutdown
```

# 8

# Interface Testing Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used for testing interfaces.

- Command List**
- “clear test interface” on page 299
  - “service test” on page 300
  - “test interface” on page 301

# clear test interface

**Overview** This command clears test results and counters after issuing a test interface command. Test results and counters must be cleared to issue subsequent test interface commands later on.

**Syntax** `clear test interface {<port-list>|all}`

| Parameter                      | Description                                                                                                                                                                                                                                                                                                                  |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;port-list&gt;</code> | The ports to test. A port-list can be: <ul style="list-style-type: none"><li>• a switch port (e.g. port1.0.6)</li><li>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-port1.0.6</li><li>• a comma-separated list of the above, e.g. port1.0.1, port1.0.5-1.0.6</li></ul> The specified ports must exist. |
| <code>all</code>               | All interfaces                                                                                                                                                                                                                                                                                                               |

**Mode** Privileged Exec

**Examples** To clear the counters for port1.0.1 use the command:

```
awplus# clear test interface port1.0.1
```

To clear the counters for all interfaces use the command:

```
awplus# clear test interface all
```

**Related Commands** [test interface](#)

## service test

**Overview** This command puts the device into the interface testing state, ready to begin testing. After entering this command, enter Interface Configuration mode for the desired interfaces and enter the command [test interface](#).

Do not test interfaces on a device that is part of a live network—disconnect the device first.

Use the **no** variant of this command to stop the test service.

**Syntax** service test  
no service test

**Mode** Global Configuration

**Example** To put the device into a test state, use the command:

```
awplus(config)# service test
```

**Related  
Commands** [test interface](#)

# test interface

**Overview** This command starts a test on a port or all ports or a selected range or list of ports.

Use the **no** variant of this command to disable this function. The test duration can be configured by specifying the time in minutes after specifying a port or ports to test.

For an example of all the commands required to test switch ports, see the Examples section in this command. To test the Eth port, set its speed to 100 by using the command **speed 100**.

**NOTE:** Do not run test interface on live networks because this will degrade network performance.

**Syntax** test interface {<port-list>|all} [time{<1-60>|cont}]  
no test interface {<port-list>|all}

| Parameter   | Description                                                                                                                                                                                                                                                                                                                  |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <port-list> | The ports to test. A port-list can be: <ul style="list-style-type: none"><li>• a switch port (e.g. port1.0.6)</li><li>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-port1.0.6</li><li>• a comma-separated list of the above, e.g. port1.0.1, port1.0.5-1.0.6</li></ul> The specified ports must exist. |
| all         | All ports                                                                                                                                                                                                                                                                                                                    |
| time        | Keyword entered prior to the value for the time duration of the interface test.                                                                                                                                                                                                                                              |
| <1-60>      | Specifies duration of time to test the interface or interfaces in minutes (from a minimum of 1 minute to a maximum of 60 minutes). The default is 4 minutes.                                                                                                                                                                 |
| cont        | Specifies continuous interface testing until canceled with command negation.                                                                                                                                                                                                                                                 |

**Mode** Privileged Exec

**Example** To test the switch ports in VLAN 1, install loopbacks in the ports, and enter the following commands:

```
awplus(config)# service test
awplus(config)# no spanning-tree rstp enable bridge-forward
awplus(config)# interface vlan1
awplus(config-if)# shutdown
awplus(config-if)# end
awplus# test interface all
```

To see the output, use the commands:

```
awplus# show test
```

```
awplus# show test count
```

To start the test on all interfaces for 1 minute use the command:

```
awplus# test interface all time 1
```

**Related  
Commands**   [clear test interface](#)

# 9

# Alarm Monitoring Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure alarm monitoring. For more information, see the [Alarm Monitoring Feature Overview and Configuration Guide](#).

- Command List**
- “[alarm facility](#)” on page 304
  - “[show alarm settings](#)” on page 307
  - “[show facility-alarm status](#)” on page 308

# alarm facility

**Overview** Use this command to enable alarm monitoring. Alarm monitoring is user-configured, including which alarms are enabled, and the LED and relay settings for each alarm.

Use the **no** variant of this command to disable the alarm facility for a particular alarm.

The command syntax varies depending on the type of alarm you are configuring. The section below includes the syntax for each alarm type.

**Syntax**

```
alarm facility epsr {led|relay}
alarm facility input-alarm <input-alarm-number> {alarm-position
{open|close}|led|relay}
alarm facility link-down <port-list> {led|relay}
alarm facility loopprot {led|relay}
alarm facility main-pse {led|relay}
alarm facility power-supply <power-supply-number> {led|relay}
alarm facility pse-port <port-list> {led|relay}
alarm facility temperature {led|relay}
no alarm facility {epsr|input-alarm <number>|link-aggregation
{partial-failure|total-failure}|link-down
<port-list>|loopprot|main-pse|power-supply <id>|pse-port
<port-list>|temperature} {led|relay}
```

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                  |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| epsr                 | EPSR alarm                                                                                                                                                                                                                                                                                                                                                                   |
| input-alarm          | External contact input alarm.                                                                                                                                                                                                                                                                                                                                                |
| <input-alarm-number> | The external contact input number. The current models have only a single pair of input contacts, so this number must be 1.                                                                                                                                                                                                                                                   |
| link-down            | Link failure alarm. A link is down on a particular switch port.                                                                                                                                                                                                                                                                                                              |
| <port-list>          | The switch ports on which the alarm will be activated or disabled. The port list can be any of the following: <ul style="list-style-type: none"><li>• An individual port. Example: 1.0.3</li><li>• A continuous range of ports. Example: 1.0.1-1.0.3</li><li>• A combination of individual ports and port ranges, separated by commas. Example: 1.0.1, 1.0.3-1.0.4</li></ul> |
| loopprot             | Loop protection alarm.                                                                                                                                                                                                                                                                                                                                                       |



| Parameter             | Description                                                                                                                                                                                                |
|-----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| main-pse              | Main power source equipment failure alarm. The sum of the power consumed by all of the PoE devices plugged into the switch exceeds the maximum permitted.<br>Note: This alarm pertains to PoE models only. |
| power-supply          | Power supply failure alarm. The designated power supply is down.                                                                                                                                           |
| <power-supply-number> | The power supply unit number. The switch has two power supplies, so the number must be 1 or 2.                                                                                                             |
| pse-port              | PoE failure on a switch port alarm. A PoE device plugged into a port is consuming more than the maximum power output for the port.                                                                         |
| temperature           | High temperature alarm. If enabled, this alarm is triggered when the temperature of the device exceeds 95 degrees Celsius.                                                                                 |
| led                   | Enable or disable the LED for the alarm.                                                                                                                                                                   |
| relay                 | Enable or disable the relay output for the alarm.                                                                                                                                                          |
| alarm-position        | The position (open or closed) of the input contact corresponding to the alarm that has occurred.                                                                                                           |
| open                  | The electrical circuit for the contact input is open.                                                                                                                                                      |
| close                 | The electrical circuit for the contact input is closed.                                                                                                                                                    |

**Default** All alarms are disabled by default.

**Mode** Global Configuration

**Usage** Enabling alarms allows you to monitor the switch environment and respond to problems as they occur.

**Example** To turn on the LED in case a loop occurs, use the command:

```
awplus# configure terminal
awplus(config)# alarm facility looprot led
```

To have an alarm when the contact input is open, use the command:

```
awplus# configure terminal
awplus(config)# alarm facility input-alarm 1 alarm-position
open
```

To turn off the led from flashing when the device temperature is too high, use the command:

```
awplus# configure terminal
awplus(config)# no alarm facility temperature led
```

**Related  
Commands**    [show alarm settings](#)  
                  [show facility-alarm status](#)

# show alarm settings

**Overview** Use this command to view all alarms configured on the switch. The output also includes the alarm position for each contact input.

**Syntax** show alarm settings

**Mode** User Exec and Privileged Exec

**Example** To display all of the alarm settings enabled on the switch, use the command:

```
awplus# show alarm settings
```

**Output** Figure 9-1: Example output from the **show alarm settings** command

| Alarm                  | ID        | LED            | Relay    |
|------------------------|-----------|----------------|----------|
| -----                  | -----     | -----          | -----    |
| External PSU           | 1         | Enabled        | Disabled |
| External PSU           | 2         | Enabled        | Disabled |
| EPSR                   | -         | Disabled       | Disabled |
| External contact input | 1         | Disabled       | Disabled |
| Link down              | port1.0.1 | Disabled       | Disabled |
| Link down              | port1.0.2 | Disabled       | Disabled |
| Link down              | port1.0.3 | Disabled       | Disabled |
| Link down              | port1.0.4 | Disabled       | Disabled |
| Link down              | port1.0.5 | Disabled       | Disabled |
| Link down              | port1.0.6 | Disabled       | Disabled |
| Loop detect            | -         | Disabled       | Enabled  |
| Main PSE failure       | -         | Disabled       | Disabled |
| PoE failure            | port1.0.1 | Disabled       | Disabled |
| PoE failure            | port1.0.2 | Disabled       | Disabled |
| PoE failure            | port1.0.3 | Disabled       | Disabled |
| PoE failure            | port1.0.4 | Disabled       | Disabled |
| Temperature            | -         | Enabled        | Enabled  |
| Alarm                  | ID        | Alarm position |          |
| -----                  | -----     | -----          |          |
| External contact input | 1         | Open           |          |

**Related Commands** [alarm facility](#)  
[show facility-alarm status](#)

# show facility-alarm status

**Overview** Use this command to view all of the alarms that are currently active on the switch.

**Syntax** show facility-alarm status

**Mode** User Exec and Privileged Exec

**Example** To display all of the currently active alarms on the switch, use the command:

```
awplus# show facility-alarm status
```

**Output** Figure 9-2: Example output from the **show facility-alarm status** command

| Active alarms | ID        |
|---------------|-----------|
| -----         | -----     |
| External PSU  | 2         |
| EPSR          | -         |
| Link down     | port1.0.1 |
| PoE failure   | port1.0.1 |

**Related  
Commands** [alarm facility](#)  
[show alarm settings](#)

# 10

# Switching Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure switching.

For more information, see the [Switching Feature Overview and Configuration Guide](#).

- Command List**
- “[backpressure](#)” on page 311
  - “[clear loop-protection counters](#)” on page 313
  - “[clear mac address-table static](#)” on page 314
  - “[clear mac address-table dynamic](#)” on page 315
  - “[clear port counter](#)” on page 317
  - “[debug loopprot](#)” on page 318
  - “[debug platform packet](#)” on page 319
  - “[duplex](#)” on page 321
  - “[flowcontrol \(switch port\)](#)” on page 322
  - “[linkflap action](#)” on page 324
  - “[loop-protection](#)” on page 325
  - “[loop-protection action](#)” on page 326
  - “[loop-protection action-delay-time](#)” on page 327
  - “[loop-protection timeout](#)” on page 328
  - “[mac address-table acquire](#)” on page 329
  - “[mac address-table ageing-time](#)” on page 330
  - “[mac address-table static](#)” on page 331
  - “[mirror interface](#)” on page 332

- [“platform stop-unreg-mc-flooding”](#) on page 334
- [“platform vlan-stacking-tpid”](#) on page 336
- [“polarity”](#) on page 337
- [“show debugging loopprot”](#) on page 338
- [“show debugging platform packet”](#) on page 339
- [“show flowcontrol interface”](#) on page 340
- [“show interface err-disabled”](#) on page 341
- [“show interface switchport”](#) on page 342
- [“show loop-protection”](#) on page 343
- [“show mac address-table”](#) on page 344
- [“show mirror”](#) on page 346
- [“show mirror interface”](#) on page 347
- [“show platform”](#) on page 348
- [“show platform classifier statistics utilization brief”](#) on page 349
- [“show platform port”](#) on page 350
- [“speed”](#) on page 354
- [“undebg loopprot”](#) on page 356
- [“undebg platform packet”](#) on page 357

# backpressure

**Overview** This command provides a method of applying flow control to ports running in half duplex mode. The setting will only apply when the link is in the half-duplex state.

You can disable backpressure on an interface using the **off** parameter or the **no** variant of this command.

**Syntax** backpressure {on|off}  
no backpressure

| Parameters | Description                        |
|------------|------------------------------------|
| on         | Enables half-duplex flow control.  |
| off        | Disables half-duplex flow control. |

**Default** Backpressure is turned off by default. You can determine whether an interface has backpressure enabled by viewing the running-config output; **backpressure on** is shown for interfaces if this feature is enabled.

**Mode** Interface Configuration

**Usage** The backpressure feature enables half duplex Ethernet ports to control traffic flow during congestion by preventing further packets arriving. Back pressure utilizes a pre-802.3x mechanism in order to apply Ethernet flow control to switch ports that are configured in the half duplex mode.

The flow control applied by the [flowcontrol \(switch port\)](#) command operates only on full-duplex links, whereas back pressure operates only on half-duplex links.

If a port has insufficient capacity to receive further frames, the device will simulate a collision by transmitting a CSMA/CD jamming signal from this port until the buffer empties. The jamming signal causes the sending device to stop transmitting and wait a random period of time, before retransmitting its data, thus providing time for the buffer to clear. Although this command is only valid for switch ports operating in half-duplex mode the remote device (the one sending the data) can be operating in the full duplex mode.

To see the currently-negotiated duplex mode for ports whose links are up, use the command [show interface](#). To see the configured duplex mode (when different from the default), use the command [show running-config](#).

**Examples** To enable back pressure flow control on interfaces port1.0.1-port1.0.2 enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# backpressure on
```

To disable back pressure flow control on interface port1.0.2 enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# backpressure off
```

**Validation  
Commands**    [show running-config](#)  
                  [show interface](#)

**Related  
Commands**    [duplex](#)



# clear loop-protection counters

**Overview** Use this command to clear the counters for the Loop Protection counters.

**Syntax** `clear loop-protection [interface <port-list>] counters`

| Parameters  | Description                                     |
|-------------|-------------------------------------------------|
| interface   | The interface whose counters are to be cleared. |
| <port-list> | A port, a port range, or an aggregated link.    |

**Mode** Privileged Exec

**Examples** To clear the counter information for all interfaces:

```
awplus# clear loop-protection counters
```

To clear the counter information for a single port:

```
awplus# clear loop-protection interface port1.0.1 counters
```

# clear mac address-table static

**Overview** Use this command to clear the filtering database of all statically configured entries for a selected MAC address, interface, or VLAN.

**Syntax** `clear mac address-table static [address <mac-address>|interface <port>|vlan <vid>]`

| Parameter     | Description                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| address       | Specify a MAC (Media Access Control) address to be cleared from the filtering database.                                                                                                                  |
| <mac-address> | Enter a MAC address to be cleared from the database in the format HHHH.HHHH.HHHH.                                                                                                                        |
| interface     | Specify a switch port to be cleared from the filtering database.                                                                                                                                         |
| <port>        | Specify the switch port from which address entries will be cleared. This can be a single switch port, (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |
| vlan          | Specify a VLAN to be cleared from the filtering database.                                                                                                                                                |
| <vid>         | Enter a VID (VLAN ID) in the range <1 - 4094> to be cleared from the filtering database.                                                                                                                 |

**Mode** Privileged Exec

**Usage** Use this command with options to clear the filtering database of all entries made from the CLI for a given MAC address, interface or VLAN. Use this command without options to clear any entries made from the CLI.

Compare this usage with [clear mac address-table dynamic](#) command.

**Examples** This example shows how to clear all filtering database entries configured through the CLI.

```
awplus# clear mac address-table static
```

This example shows how to clear all filtering database entries for a given interface configured through the CLI.

```
awplus# clear mac address-table static interface port1.0.3
```

This example shows how to clear filtering database entries filtering database entries configured through the CLI for a given mac address.

```
awplus# clear mac address-table static address 0202.0202.0202
```

**Related Commands** [clear mac address-table dynamic](#)  
[mac address-table static](#)  
[show mac address-table](#)

# clear mac address-table dynamic

**Overview** Use this command to clear the filtering database of all entries learned for a selected MAC address, an MSTP instance, a switch port interface or a VLAN interface.

**Syntax** `clear mac address-table dynamic [address <mac-address>|interface <port> [instance <inst>]]vlan <vid>]`

| Parameter     | Description                                                                                                                                                                                              |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface     | Specify a switch port to be cleared from the filtering database.                                                                                                                                         |
| <port>        | Specify the switch port from which address entries will be cleared. This can be a single switch port, (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |
| address       | Specify a MAC (Media Access Control) address to be cleared from the filtering database.                                                                                                                  |
| <mac-address> | Enter a MAC address to be cleared from the database in the format HHHH.HHHH.HHHH.                                                                                                                        |
| instance      | Specify an MSTP (Multiple Spanning Tree) instance to be cleared from the filtering database.                                                                                                             |
| <inst>        | Enter an MSTP instance in the range <1 - 63> to be cleared from the filtering database.                                                                                                                  |
| vlan          | Specify a VLAN to be cleared from the filtering database.                                                                                                                                                |
| <vid>         | Enter a VID (VLAN ID) in the range <1 - 4094> to be cleared from the filtering database.                                                                                                                 |

**Mode** Privileged Exec

**Usage** Use this command with options to clear the filtering database of all entries learned for a given MAC address, interface or VLAN. Use this command without options to clear any learned entries.

Use the optional `instance` parameter to clear the filtering database entries associated with a specified MSTP instance. Note that you must first specify a switch port interface before you can specify an MSTP instance.

Compare this usage and operation with the [clear mac address-table static](#) command. Note that an MSTP instance cannot be specified with **clear mac address-table static**.

**Examples** This example shows how to clear all dynamically learned filtering database entries for all interfaces, addresses, VLANs.

```
awplus# clear mac address-table dynamic
```

This example shows how to clear all dynamically learned filtering database entries when learned through device operation for a given MAC address.

```
awplus# clear mac address-table dynamic address 0202.0202.0202
```

This example shows how to clear all dynamically learned filtering database entries when learned through device operation for a given MSTP instance 1 on switch port interface port1.0.2.

```
awplus# clear mac address-table dynamic interface port1.0.2
instance 1
```

**Related  
Commands**

[clear mac address-table static](#)

[show mac address-table](#)

# clear port counter

**Overview** Use this command to clear the packet counters of the port.

**Syntax** clear port counter [*<port>*]

| Parameter           | Description              |
|---------------------|--------------------------|
| <i>&lt;port&gt;</i> | The port number or range |

**Mode** Privileged Exec

**Example** To clear the packet counter for port1.0.1, use the command:

```
awplus# clear port counter port1.0.1
```

**Related  
Commands** [show platform port](#)

# debug loopprot

**Overview** This command enables Loop Protection debugging.  
The **no** variant of this command disables Loop Protection debugging.

**Syntax** debug loopprot {info|msg|pkt|state|nsm|all}  
no debug loopprot {info|msg|pkt|state|nsm|all}

| Parameter | Description                                                                    |
|-----------|--------------------------------------------------------------------------------|
| info      | General Loop Protection information.                                           |
| msg       | Received and transmitted Loop Detection Frames (LDFs).                         |
| pkt       | Echo raw ASCII display of received and transmitted LDF packets to the console. |
| state     | Loop Protection states transitions.                                            |
| nsm       | Network Service Module information.                                            |
| all       | All debugging information.                                                     |

**Mode** Privileged Exec and Global Configuration

**Example** To enable debug for all state transitions, use the command:  
awplus# debug loopprot state

**Related Commands** [show debugging loopprot](#)  
[undebug loopprot](#)

# debug platform packet

**Overview** This command enables platform to CPU level packet debug functionality on the device.

Use the **no** variant of this command to disable platform to CPU level packet debug. If the result means both send and receive packet debug are disabled, then any active timeout will be canceled.

**Syntax** debug platform packet [recv] [send] [timeout <timeout>] [vlan <vlan-id>|all]

no debug platform packet [recv] [send]

| Parameter | Description                                        |
|-----------|----------------------------------------------------|
| recv      | Debug packets received.                            |
| send      | Debug packets sent.                                |
| timeout   | Stop debug after a specified time.                 |
| <timeout> | <0-3600>The timeout period, specified in seconds.  |
| vlan      | Limit debug to a single VLAN ID specified.         |
| <vlan-id> | <1-4094> The VLAN ID to limit the debug output on. |
| all       | Debug all VLANs (default setting).                 |

**Default** A 5 minute timeout is configured by default if no other timeout duration is specified.

**Mode** Privileged Exec and Global Configuration

**Usage** This command can be used to trace packets sent and received by the CPU. If a timeout is not specified, then a default 5 minute timeout will be applied.

If a timeout of 0 is specified, packet debug will be generated until the **no** variant of this command is used or another timeout value is specified. The timeout value applies to both send and receive debug and is updated whenever the **debug platform packet** command is used.

**Examples** To enable both receive and send packet debug for the default timeout of 5 minutes, enter:

```
awplus# debug platform packet
```

To enable receive packet debug for 10 seconds, enter:

```
awplus# debug platform packet recv timeout 10
```

To enable send packet debug with no timeout, enter:

```
awplus# debug platform packet send timeout 0
```

To enable VLAN packet debug for VLAN 2 with a timeout duration of 3 minutes, enter:

```
awplus# debug platform packet vlan 2 timeout 150
```

To disable receive packet debug, enter:

```
awplus# no debug platform packet recv
```

**Related  
Commands**    [show debugging platform packet](#)  
                  [undebug platform packet](#)



# duplex

**Overview** This command changes the duplex mode for the specified port.

To see the currently-negotiated duplex mode for ports whose links are up, use the command [show interface](#). To see the configured duplex mode (when different from the default), use the command [show running-config](#).

**Syntax** duplex {auto|full|half}

| Parameter | Description                       |
|-----------|-----------------------------------|
| auto      | Auto-negotiate duplex mode.       |
| full      | Operate in full duplex mode only. |
| half      | Operate in half duplex mode only. |

**Default** By default, ports auto-negotiate duplex mode (except for 100Base-FX ports which do not support auto-negotiation, so default to full duplex mode).

**Mode** Interface Configuration

**Usage** switch ports in a static or dynamic (LACP) channel group must have the same port speed and be in full duplex mode. Once switch ports have been aggregated into a channel group, you can set the duplex mode of all the switch ports in the channel group by applying this command to the channel group.

**Examples** To specify full duplex for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex full
```

To specify half duplex for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex half
```

To auto-negotiate duplex mode for port1.0.4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex auto
```

**Related Commands**

- [backpressure](#)
- [polarity](#)
- [speed](#)
- [show interface](#)

## flowcontrol (switch port)

**Overview** Use this command to enable flow control, and configure the flow control mode for the switch port.

Use the **no** variant of this command to disable flow control for the specified switch port.

**Syntax** flowcontrol {send|receive} {off|on}  
no flowcontrol

| Parameter | Description                                                                                                                                          |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| receive   | When the port receives pause frames, it temporarily stops (pauses) sending traffic.                                                                  |
| on        | Enable the specified flow control.                                                                                                                   |
| off       | Disable the specified flow control.                                                                                                                  |
| send      | When the port is congested (receiving too much traffic), it sends pause frames to request the other end to temporarily stop (pause) sending traffic. |

**Default** By default, flow control is disabled.

**Mode** Interface Configuration

**Usage** The flow control mechanism specified by 802.3x is only for full duplex links. It operates by sending PAUSE frames to the link partner to temporarily suspend transmission on the link

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion, and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When the local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the congestion period.

Flow control is not recommended when running QoS or ACLs, because the complex queuing, scheduling, and filtering configured by QoS or ACLs may be slowed by applying flow control.

For half-duplex links, an older form of flow control known as backpressure is supported. See the related [backpressure](#) command.

For flow control on async serial (console) ports, see the [flowcontrol hardware \(asyn/console\)](#) command.

**Examples**   awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# flowcontrol receive on  
awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# flowcontrol send on  
awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# flowcontrol receive off  
awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# flowcontrol send off

**Validation**   show running-config  
**Commands**

**Related**       backpressure  
**Commands**

# linkflap action

**Overview** Use this command to detect flapping on all ports. If more than 15 flaps occur in less than 15 seconds the flapping port will shut down.

Use the **no** variant of this command to disable flapping detection at this rate.

**Syntax** linkflap action [shutdown]  
no linkflap action

| Parameter | Description                       |
|-----------|-----------------------------------|
| linkflap  | Global setting for link flapping. |
| action    | Specify the action for port.      |
| shutdown  | Shutdown the port.                |

**Default** Linkflap action is disabled by default.

**Mode** Global Configuration

**Example** To enable the linkflap action command on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# linkflap action shutdown
```

# loop-protection

**Overview** Use this command to enable the loop-protection loop-detection feature, and configure the detection mechanism parameters.

Use the **no** variant of this command to disable the loop-protection loop-detection feature.

**Syntax** `loop-protection loop-detect [ldf-interval <period>]  
[ldf-rx-window <frames>] [fast-block]  
no loop-protection [loop-detect]`

| Parameter     | Description                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------|
| loop-detect   | Enables loop detection when used with loop-protection keywords. Disables loop detection when used with no loop-protection keywords. |
| ldf-interval  | The time (in seconds) between successive loop-detect frames being sent.                                                             |
| <period>      | Specify a period between 1 and 600 seconds. The default is 10 seconds.                                                              |
| ldf-rx-window | The number of transmitted loop detection frames whose details are held for comparing with frames arriving at the same port.         |
| <frames>      | Specify a value for the window size between 1 and 5 frames. The default is 3 frames.                                                |
| [fast-block]  | The fast-block blocks transmitting port to keep partial connectivity.                                                               |

**Default** The loop-protection loop-detection feature is disabled by default. The default interval is 10 seconds, and the default window size is 3 frames.

**Mode** Global Configuration

**Usage** See the “Loop Protection” section in the [Switching Feature Overview and Configuration Guide](#) for relevant conceptual, configuration, and overview information prior to applying this command.

**Example** To enable the loop-detect mechanism on the switch, and generate loop-detect frames once every 5 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# loop-protection loop-detect ldf-interval 5
```

# loop-protection action

**Overview** Use this command to specify the protective action to apply when a network loop is detected on an interface.

Use the **no** variant of this command to reset the loop protection actions to the default action, vlan-disable, on an interface.

**NOTE:** Currently the learn-disable parameter is not supported. If specified, an error message will be displayed.

**Syntax** loop-protection  
action {link-down|log-only|port-disable|vlan-disable|none}  
no loop-protection action

| Parameter    | Description                                                                                                                                                             |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| link-down    | Block all traffic on a port (or aggregated link) that detected the loop, and take <b>down</b> the link.                                                                 |
| log-only     | Details of loop conditions are logged. No action is applied to the port (or aggregated link).                                                                           |
| port-disable | Block all traffic on interface for which the loop occurred, but keep the link in the <b>up</b> state.                                                                   |
| vlan-disable | Block all traffic for the VLAN on which the loop traffic was detected. Note that setting this parameter will also enable ingress filtering. This is the default action. |
| none         | Applies no protective action.                                                                                                                                           |

**Default** loop-protection action vlan-disable

**Mode** Interface Configuration

**Usage** See the “Loop Protection” section in the [Switching Feature Overview and Configuration Guide](#) for relevant conceptual, configuration, and overview information prior to applying this command.

**Example** To disable an interface (port1.0.4), and bring the link down, when a network loop is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection action link-down
```

# loop-protection action-delay-time

**Overview** Use this command to sets the loop protection action delay time for an interface to specified values in seconds. The action delay time specifies the waiting period for the action.

Use the **no** variant of this command to reset the loop protection action delay time for an interface to default.

**Syntax** `loop-protection action-delay-time <0-86400>`  
`no loop-protection action`

| Parameter | Description                                              |
|-----------|----------------------------------------------------------|
| <0-86400> | Time in seconds; 0 means action delay timer is disabled. |

**Default** Action delay timer is disabled by default.

**Mode** Interface Configuration

**Example** To configure a loop protection action delay time of 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection action-delay-time 10
```

To reset the Loop Protection action delay time to default, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.1.4
awplus(config-if)# no loop-protection action-delay-time
```

**Related Commands** [show loop-protection](#)

# loop-protection timeout

**Overview** Use this command to specify the Loop Protection recovery action duration on an interface.

Use the **no** variant of this command to set the loop protection timeout to the default.

**Syntax** loop-protection timeout *<duration>*  
no loop-protection timeout

| Parameter               | Description                                                                                                                                                                                                      |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;duration&gt;</i> | The time (in seconds) for which the configured action will apply before being disabled. This duration can be set between 0 and 86400 seconds (24 hours). The set of 0 means infinity so timeout does not expire. |

**Default** The default is 7 seconds.

**Mode** Interface Configuration

**Usage** See the “Loop Protection” section in the [Switching Feature Overview and Configuration Guide](#) for relevant conceptual, configuration, and overview information prior to applying this command.

**Example** To configure a loop protection action timeout of 10 seconds for port1.0.4, use the command:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection timeout 10
```



# mac address-table acquire

**Overview** Use this command to enable MAC address learning on the device.

Use the **no** variant of this command to disable learning.

**Syntax** mac address-table acquire  
no mac address-table acquire

**Default** Learning is enabled by default for all instances.

**Mode** Global Configuration

**Example** awplus# configure terminal  
awplus(config)# mac address-table acquire

# mac address-table ageing-time

**Overview** Use this command to specify an ageing-out time for a learned MAC address. The learned MAC address will persist for at least the specified time.

The **no** variant of this command will reset the ageing-out time back to the default of 300 seconds (5 minutes).

**Syntax** mac address-table ageing-time *<ageing-timer>* none  
no mac address-table ageing-time

| Parameter                   | Description                                                     |
|-----------------------------|-----------------------------------------------------------------|
| <i>&lt;ageing-timer&gt;</i> | <i>&lt;10-1000000&gt;</i> The number of seconds of persistence. |
| none                        | Disable learned MAC address timeout.                            |

**Default** The default ageing time is 300 seconds.

**Mode** Global Configuration

**Examples** The following commands specify various ageing timeouts on the device:

```
awplus# configure terminal
awplus(config)# mac address-table ageing-time 1000
awplus# configure terminal
awplus(config)# mac address-table ageing-time none
awplus# configure terminal
awplus(config)# no mac address-table ageing-time
```

# mac address-table static

**Overview** Use this command to statically configure the MAC address-table to forward or discard frames with a matching destination MAC address.

**Syntax** `mac address-table static <mac-addr> {forward|discard} interface <port> [vlan <vid>]`  
`no mac address-table static <mac-addr> {forward|discard} interface <port> [vlan <vid>]`

| Parameter  | Description                                                                                                                                                             |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <mac-addr> | The destination MAC address in HHHH . HHHH . HHHH format.                                                                                                               |
| <port>     | The port to display information about. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |
| <vid>      | The VLAN ID. If you do not specify a VLAN, its value defaults to vlan 1.                                                                                                |

**Mode** Global Configuration

**Usage** The **mac address-table static** command is only applicable to Layer 2 switched traffic within a single VLAN. Do not apply the **mac address-table static** command to Layer 3 switched traffic passing from one VLAN to another VLAN. Frames will not be discarded across VLANs because packets are routed across VLANs. This command only works on Layer 2 traffic.

**Example** `awplus# configure terminal`  
`awplus(config)# mac address-table static 2222.2222.2222 forward`  
`interface port1.0.4 vlan 3`

**Related Commands** [clear mac address-table static](#)  
[show mac address-table](#)

# mirror interface

**Overview** Use this command to define a mirror port and mirrored (monitored) ports and direction of traffic to be mirrored. The port for which you enter interface mode will be the mirror port.

The destination port is removed from all VLANs, and no longer participates in other switching.

Use the **no** variant of this command to disable port mirroring by the destination port on the specified source port.

**Syntax** mirror interface <source-port-list> direction  
{both|receive|transmit}  
no mirror interface <source-port-list>

| Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                            |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <source-port-list> | The source switch ports to mirror. A port-list can be: <ul style="list-style-type: none"><li>• a port (e.g. port1.0.2)</li><li>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.2</li><li>• a comma-separated list of ports and port ranges, e.g. port1.0.1, port1.0.4-1.0.6</li></ul> The source port list cannot include dynamic or static channel groups (link aggregators). |
| direction          | Specifies whether to mirror traffic that the source port receives, transmits, or both.                                                                                                                                                                                                                                                                                                                 |
| both               | Mirroring traffic both received and transmitted by the source port.                                                                                                                                                                                                                                                                                                                                    |
| receive            | Mirroring traffic received by the source port.                                                                                                                                                                                                                                                                                                                                                         |
| transmit           | Mirroring traffic transmitted by the source port.                                                                                                                                                                                                                                                                                                                                                      |

**Mode** Interface Configuration

**Usage** Use this command to send traffic to another device connected to the mirror port for monitoring.

See the “Port Mirroring” section in the [Switching Feature Overview and Configuration Guide](#) for more information.

A mirror port cannot be associated with a VLAN. If a switch port is configured to be a mirror port, it is automatically removed from any VLAN it was associated with.

This command can only be applied to a single mirror (destination) port, not to a range of ports, nor to a static or dynamic channel group. Do not apply multiple interfaces with an interface command before issuing the mirror interface command. One interface may have multiple mirror interfaces.

**Example** To mirror traffic received and transmitted on port1.0.4 and port1.0.5 to destination port1.0.3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# mirror interface port1.0.4,port1.0.5
direction both
```

**Related  
Commands** [access-list \(hardware IP numbered\)](#)  
[access-list \(hardware MAC numbered\)](#)  
[default-action](#)

# platform stop-unreg-mc-flooding

**Overview** This command stops multicast packets flooding out of all the ports in the VLAN until these packets are registered. This command does this by dropping unknown multicast packets. Unregistered traffic will not flow until the switch has registered it, regardless of attempts to subscribe to it. Once the traffic is registered, it flows to registered subscribers and ports.

Use the **no** variant of this command to revert to default behavior and disable this feature.

**NOTE:** *This command should not be used within any IPv6 networks.*

*IPv6 neighbor discovery operation is inhibited by this feature.*

*This command does not stop reserved Local Network Control Block IPv4 multicast packets in the address range 224.0.0.1 to 224.0.0.255 (224.0.0/24).*

See

[www.iana.org/assignments/multicast-addresses/multicast-addresses.xml#multicast-addresses-1](http://www.iana.org/assignments/multicast-addresses/multicast-addresses.xml#multicast-addresses-1)

**Syntax** platform stop-unreg-mc-flooding  
no platform stop-unreg-mc-flooding

**Default** This feature is disabled by default.

**Mode** Global Configuration

**Usage** This command stops the periodic flooding of unknown or unregistered multicast packets when the Group Membership interval timer expires and there are no subscribers to a multicast group. If there is multicast traffic in a VLAN without subscribers, multicast traffic temporarily floods out of the VLAN when the Group Membership interval timer expires, which happens when the switch does not get replies from Group Membership queries.

This command also stops the initial flood of multicast packets that happens when a new multicast source starts to send traffic. This flooding lasts until snooping recognizes the multicast group. For example, in sites where IP cameras have multicast groups, traffic is flooded to the VLAN and causes large bursts of traffic. Use this command when there is limited processing available for large bursts of traffic, such as in sites with IP cameras.

**Output** See the console message warning about IPv6 operation after entering this command:

```
% WARNING: IPv6 will not work with this setting enabled
% Please consult the documentation for more information
```

See these sample console messages when the Group Membership interval timer expires, which happens when the switch does not get replies from Group Membership queries:

```
awplus: [MLD-EVENTS] Grp - Rec Liveness Timer: Expiry for Grp ff0e::1 on port1.2.7
awplus: [IGMP-EVENTS] : Expiry (Unreg MC Timer) for Grp 224.2.2.2 on vlan4
```

**Examples** To enable this feature and stop multicast packet flooding, use the following commands:

```
awplus# configure terminal
awplus(config)# platform stop-unreg-mc-flooding
```

To disable this feature and allow multicast packet flooding, use the following commands:

```
awplus# configure terminal
awplus(config)# no platform stop-unreg-mc-flooding
```

**Related  
Commands** [show platform](#)  
[show running-config](#)

# platform vlan-stacking-tpid

**Overview** This command specifies the Tag Protocol Identifier (TPID) value that applies to all frames that are carrying double tagged VLANs. All nested VLANs must use the same TPID value. (This feature is sometimes referred to as VLAN stacking or VLAN double-tagging.)

Use the **no** variant of this command to revert to the default TPID value (0x8100).

**Syntax** platform vlan-stacking-tpid <tpid>  
no platform vlan-stacking-tpid

| Parameter | Description                                                               |
|-----------|---------------------------------------------------------------------------|
| <tpid>    | The Ethernet type of the tagged packet, as a two byte hexadecimal number. |

**Default** The default TPID value is 0x8100.

**Mode** Global Configuration

**Examples** To set the VLAN stacking TPID value to 0x9100, use the following commands:

```
awplus# configure terminal
awplus(config)# platform vlan-stacking-tpid 9100
```

To reset the VLAN stacking TPID value to the default (0x8100), use the following commands:

```
awplus# configure terminal
awplus(config)# no platform vlan-stacking-tpid
```

**Related Commands** [switchport vlan-stacking \(double tagging\)](#)  
[show platform](#)  
[show running-config](#)



# polarity

**Overview** This command sets the MDI/MDIX polarity on a copper-based switch port.

**Syntax** `polarity {auto|mdi|mdix}`

| Parameter | Description                                                                  |
|-----------|------------------------------------------------------------------------------|
| mdi       | Sets the polarity to MDI (medium dependent interface).                       |
| mdix      | Sets the polarity to MDI-X (medium dependent interface crossover).           |
| auto      | The switch port sets the polarity automatically. This is the default option. |

**Default** By default, switch ports set the polarity automatically (**auto**).

**Mode** Interface Configuration

**Usage** We recommend the default **auto** setting for MDI/MDIX polarity. Polarity applies to copper 10BASE-T, 100BASE-T, and 1000BASE-T switch ports; It does not apply to fiber ports. See the “MDI/MDIX Connection Modes” section in the [Switching Feature Overview and Configuration Guide](#) for more information.

**Example** To set the polarity for port1.0.6 to fixed MDI mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# polarity mdi
```

# show debugging loopprot

**Overview** This command shows Loop Protection debugging information.

**Syntax** show debugging loopprot

**Mode** User Exec and Privileged Exec

**Example** To display the enabled Loop Protection debugging modes, use the command:

```
awplus# show debugging loopprot
```

**Related  
Commands** [debug loopprot](#)

# show debugging platform packet

**Overview** This command shows platform to CPU level packet debugging information.

**Syntax** show debugging platform packet

**Mode** User Exec and Privileged Exec

**Example** To display the platform packet debugging information, use the command:

```
awplus# show debugging platform packet
```

**Related  
Commands** [debug platform packet](#)  
[undebug platform packet](#)

# show flowcontrol interface

**Overview** Use this command to display flow control information.

**Syntax** show flowcontrol interface <port>

| Parameter | Description                                     |
|-----------|-------------------------------------------------|
| <port>    | Specifies the name of the port to be displayed. |

**Mode** User Exec and Privileged Exec

**Example** To display the flow control for the port1.0.5, use the command:

```
awplus# show flowcontrol interface port1.0.5
```

**Output** Figure 10-1: Example output from the **show flowcontrol interface** command for a specific interface

| Port      | Send<br>admin | FlowControl<br>oper | Receive<br>admin | FlowControl<br>oper | RxPause | TxPause |
|-----------|---------------|---------------------|------------------|---------------------|---------|---------|
| -----     | -----         | -----               | -----            | -----               | -----   | -----   |
| port1.0.5 | on            | on                  | on               | on                  | 0       | 0       |

# show interface err-disabled

**Overview** Use this command to show the ports which have been dynamically shut down by protocols running on the device and the protocols responsible for the shutdown.

**Syntax** `show interface [<IFRANGE> err-disabled]`

| Parameter    | Description                                        |
|--------------|----------------------------------------------------|
| <IFRANGE>    | Interface range                                    |
| err-disabled | Brief summary of interfaces shut down by protocols |

**Mode** User Exec and Privileged Exec

**Example** Show the protocols that have shut down port2.0.21 and port2.0.23, use the commands:

```
awplus# show interface err-disabled
```

**Output** Figure 10-2: Example output from the **show interface err-disabled** command

```
awplus#show interface err-disabled
Interface Reason
port2.0.21 loop protection
port2.0.23 loop protection
```

# show interface switchport

**Overview** Use this command to show VLAN information about each switch port.

**Syntax** show interface switchport

**Mode** User Exec and Privileged Exec

**Example** To display VLAN information about each switch port, enter the command:

```
awplus# show interface switchport
```

**Output** Figure 10-3: Example output from the **show interface switchport** command

```
Interface name : port1.0.1
Switchport mode : access
Ingress filter : enable
Acceptable frame types : all
Default Vlan : 2
Configured Vlans : 2

Interface name : port1.0.2
Switchport mode : trunk
Ingress filter : enable
Acceptable frame types : all
Default Vlan : 1
Configured Vlans : 1 4 5 6 7 8
...
```

**Related Commands** [show interface memory](#)

# show loop-protection

**Overview** Use this command to display the current loop protection setup for the device.

**Syntax** `show loop-protection [interface <port-list>] [counters]`

| Parameter   | Description                                       |
|-------------|---------------------------------------------------|
| interface   | The interface selected for display.               |
| <port-list> | A port, a port range, or an aggregated link.      |
| counters    | Displays counter information for loop protection. |

**Mode** User Exec and Privileged Exec

**Usage** This command is used to display the current configuration and operation of the Loop Protection feature

**Examples** To display the current configuration status for port1.0.1, use the command:

```
awplus# show loop-protection interface port1.0.1
```

Figure 10-4: Example output from the **show loop-protection** command

|                    |              |
|--------------------|--------------|
| Loop-Detection:    | Enabled      |
| LDF Interval:      | 10 [sec]     |
| Interface:         | port1.0.1    |
| Action:            | port-disable |
| Timeout:           | 300 [sec]    |
| Vlan:              | 1            |
| Status:            | Blocking     |
| Timeout Remaining: | 115 [sec]    |
| Vlan:              | 2            |
| Status:            | Normal       |
| Timeout Remaining: | 0 [sec]      |

To display the counter information for port1.0.1, use the command:

```
awplus# show loop-protection interface port1.0.1 counters
```

Figure 10-5: Example output from the **show loop-protection interface counters** command for port1.0.1

|                 |           |
|-----------------|-----------|
| Interface:      | port1.0.1 |
| Vlan:           | 1         |
| LDF Tx:         | 3         |
| LDF Rx:         | 1         |
| Invalid LDF Rx: | 1         |
| Action:         | 1         |
| Vlan:           | 2         |
| LDF Tx:         | 3         |
| LDF Rx:         | 0         |
| Invalid LDF Rx: | 0         |
| Action:         | 0         |

# show mac address-table

**Overview** Use this command to display the mac address-table for all configured VLANs.

**Syntax** show mac address-table

**Mode** User Exec and Privileged Exec

**Usage** The **show mac address-table** command is only applicable to view a mac address-table for Layer 2 switched traffic within VLANs.

**Example** To display the mac address-table, use the following command:

```
awplus# show mac address-table
```

**Output** See the below sample output captured when there was no traffic being switched:

```
awplus#show mac address-table
```

| VLAN | Port    | MAC            | State  |
|------|---------|----------------|--------|
| 1    | unknown | 0000.cd28.0752 | static |
| ARP  | -       | 0000.cd00.0000 | static |

See the sample output captured when packets were switched and mac addresses were learned:

```
awplus#show mac address-table
```

| VLAN | Port      | MAC            | State   |
|------|-----------|----------------|---------|
| 1    | unknown   | 0000.cd28.0752 | static  |
| 1    | port1.0.6 | 0030.846e.9bf4 | dynamic |
| 1    | port1.0.4 | 0030.846e.bac7 | dynamic |
| ARP  | -         | 0000.cd00.0000 | static  |

Note the new mac addresses learned for port1.0.4 and port1.0.6 added as dynamic entries.

Note the first column of the output below shows VLAN IDs if multiple VLANs are configured:

```
awplus#show mac address-table
```

| VLAN | Port      | MAC            | State   |
|------|-----------|----------------|---------|
| 1    | unknown   | 0000.cd28.0752 | static  |
| 1    | port1.0.4 | 0030.846e.bac7 | dynamic |
| 2    | unknown   | 0000.cd28.0752 | static  |
| 2    | port1.0.6 | 0030.846e.9bf4 | dynamic |
| ARP  | -         | 0000.cd00.0000 | static  |



Also note manually configured static mac-addresses are shown to the right of the type column:

```
awplus(config)#mac address-table static 0000.1111.2222 for int
port1.0.3 vlan 2
awplus(config)#end
awplus#
awplus#show mac address-table
```

| VLAN | Port      | MAC            | State   |
|------|-----------|----------------|---------|
| 1    | unknown   | 0000.cd28.0752 | static  |
| 1    | port1.0.2 | 0030.846e.bac7 | dynamic |
| 2    | port1.0.3 | 0000.1111.2222 | static  |
| 2    | unknown   | 0000.cd28.0752 | static  |
| 2    | port1.0.5 | 0030.846e.9bf4 | dynamic |
| ARP  | -         | 0000.cd00.0000 | statics |

**Related  
Commands**

- [clear mac address-table dynamic](#)
- [clear mac address-table static](#)
- [mac address-table static](#)

# show mirror

**Overview** Use this command to display the status of all mirrored ports.

**Syntax** show mirror

**Mode** User Exec and Privileged Exec

**Example** To display the status of all mirrored ports, use the following command:

```
awplus# show mirror
```

**Output** Figure 10-6: Example output from the **show mirror** command

```
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.2
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.4
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.1
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.3
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: transmit
Monitored Port Name: port1.0.4
```

# show mirror interface

**Overview** Use this command to display port mirroring configuration for a mirrored (monitored) switch port.

**Syntax** show mirror interface *<port>*

| Parameter           | Description                                             |
|---------------------|---------------------------------------------------------|
| <i>&lt;port&gt;</i> | The monitored switch port to display information about. |

**Mode** User Exec, Privileged Exec and Interface Configuration

**Example** To display port mirroring configuration for the port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# show mirror interface port1.0.4
```

**Output** Figure 10-7: Example output from the **show mirror interface** command

```
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.4
```

# show platform

**Overview** This command displays the settings configured by using the **platform** commands.

**Syntax** show platform

**Mode** Privileged Exec

**Usage** This command displays the settings in the running config. For changes in some of these settings to take effect, the device must be rebooted with the new settings in the startup config.

**Example** To check the settings configured with **platform** commands on the device, use the following command:

```
awplus# show platform
```

**Output** Figure 10-8: Example output from the **show platform** command

```
awplus#show platform

MAC vlan hashing algorithm unknown
stop-unreg-mc-flooding off
Jumboframe support off
Vlan-stacking TPID 0x8100
Hardware Filter Size ipv4-limited-ipv6
```

Table 10-1: Parameters in the output of the **show platform** command

| Parameter                  | Description                                                                                                                                     |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|
| Jumboframe support         | Whether the jumbo frames setting is enabled or disabled.                                                                                        |
| Vlan-stacking TPID         | The value of the TPID set in the Ethernet type field when a frame has a double VLAN tag ( <a href="#">platform vlan-stacking-tpid</a> command). |
| MAC vlan hashing algorithm | MAC based VLAN hash control.                                                                                                                    |

# show platform classifier statistics utilization brief

**Overview** This command displays the number of used entries available for various platform functions, and the percentage that number of entries represents of the total available.

**Syntax** show platform classifier statistics utilization brief

**Mode** Privileged Exec

**Example** To display the platform classifier utilization statistics, use the following command:  
awplus# show platform classifier statistics utilization brief

**Output** Figure 10-9: Output from the **show platform classifier statistics utilization brief** command

```
awplus#show platform classifier statistics utilization brief

[Instance 0]
 Number of Entries:
 Policy Type Group ID Used / Total

 ACL 1476395009 0 / 118 (0%)
 Web Auth Inactive 0 / 0 (0%)
 QoS 0 / 128 (0%)
```

**Related Commands** [show platform](#)

# show platform port

**Overview** This command displays the various port registers or platform counters for specified switchports.

**Syntax** `show platform port [<port-list>|counters]`

| Parameter   | Description                                                                                                                                                                                                                                                                       |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <port-list> | The ports to display information about. A port-list can be: <ul style="list-style-type: none"><li>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.6</li><li>• a comma-separated list of ports and port ranges, e.g. port1.0.1, port1.0.4-1.0.6.</li></ul> |
| counters    | Show the platform counters.                                                                                                                                                                                                                                                       |

**Mode** Privileged Exec

**Examples** To display port registers for port1.0.1 and port1.0.2 use the following command:

```
awplus# show platform port port1.0.1-port1.0.2
```

To display platform counters for port1.0.1 and port1.0.2 use the following command:

```
awplus# show platform port port1.0.1-port1.0.2 counters
```

**Output** Figure 10-10: Example output from the **show platform port** command

```
awplus#show platform port port1.0.1
Phy register value for port1.0.1 (ifindex: 5001)

00:1140 01:7949 02:0020 03:60B1 04:01E1 05:0000 06:0004 07:2001
08:0000 09:0600 10:0000 11:0000 12:0000 13:0000 14:0000 15:0000
16:0000 17:0000 18:0000 19:0000 20:0000 21:0000 22:0000 23:0000
24:0000 25:0000 26:0000 27:0000 28:0000 29:0000 30:0000 31:0000

Port configuration for lport 0x08001000:
 enabled: 1
 loopback: 0
 link: 0
 speed: 0 max speed: 1000
 duplex: 0
 linkscan: 2
 autonegotiate: 1
 master: 2
 tx pause: 1 rx pause: 1
 untagged vlan: 1
 vlan filter: 3
 stp state: 1
 learn: 5
 discard: 0
 max frame size: 1522
 MC Disable SA: no
 MC Disable TTL: no
 MC egress untag: 0
 MC egress vid: 0
 MC TTL threshold: -1
```

Table 10-2: Parameters in the output from the **show platform port** command

| Parameter                                                   | Description                                                    |
|-------------------------------------------------------------|----------------------------------------------------------------|
| <b>Ethernet MAC counters</b>                                |                                                                |
| Combined receive/transmit packets by size (octets) counters | Number of packets in each size range received and transmitted. |
| 64                                                          | Number of 64 octet packets received and transmitted.           |
| 65 - 127                                                    | Number of 65 - 127 octet packets received and transmitted.     |
| 128 - 255                                                   | Number of 128 - 255 octet packets received and transmitted.    |
| 256 - 511                                                   | Number of 256 - 511 octet packets received and transmitted.    |
| 512 - 1023                                                  | Number of 512 - 1023 octet packets received and transmitted.   |

Table 10-2: Parameters in the output from the **show platform port** command

| Parameter               | Description                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------|
| 1024 - MaxPktSz         | Number of packets received and transmitted with size 1024 octets to the maximum packet length. |
| 1519 - 1522             | Number of 1519 - 1522 octet packets received and transmitted.                                  |
| 1519 - 2047             | Number of 1519 - 2047 octet packets received and transmitted.                                  |
| 2048 - 4095             | Number of 2048 - 4095 octet packets received and transmitted.                                  |
| 4096 - 9216             | Number of 4096 - 9216 octet packets received and transmitted.                                  |
| <b>General Counters</b> |                                                                                                |
| Receive                 | Counters for traffic received.                                                                 |
| Octets                  | Number of octets received.                                                                     |
| Pkts                    | Number of packets received.                                                                    |
| FCSErrors               | Number of FCS (Frame Check Sequence) error events received.                                    |
| UnicastPkts             | Number of unicast packets received.                                                            |
| MulticastPkts           | Number of multicast packets received.                                                          |
| BroadcastPkts           | Number of broadcast packets received.                                                          |
| PauseMACCtlFrms         | Number of Pause MAC Control Frames received.                                                   |
| OversizePkts            | Number of oversize packets received.                                                           |
| Fragments               | Number of fragments received.                                                                  |
| Jabbers                 | Number of jabber frames received.                                                              |
| UnsupportOpcode         | Number of MAC Control frames with unsupported opcode received.                                 |
| AlignmentErrors         | Receive Alignment Error Frame Counter.                                                         |
| SysErDurCarrier         | Receive Code Error Counter.                                                                    |
| CarrierSenseErr         | Receive False Carrier Counter.                                                                 |
| UndersizePkts           | Number of undersized packets received.                                                         |
| Transmit                | Counters for traffic transmitted.                                                              |



Table 10-2: Parameters in the output from the **show platform port** command

| Parameter                     | Description                                     |
|-------------------------------|-------------------------------------------------|
| Octets                        | Number of octets transmitted.                   |
| Pkts                          | Number of packets transmitted.                  |
| UnicastPkts                   | Number of unicast packets transmitted.          |
| MulticastPkts                 | Number of multicast packets transmitted.        |
| BroadcastPkts                 | Number of broadcast packets transmitted.        |
| PauseMACCtlFrms               | Number of Pause MAC Control Frames transmitted. |
| OversizePkts                  | Number of oversize packets transmitted.         |
| FrameWDeferrdTx               | Transmit Single Deferral Frame counter.         |
| FrmWExcesDefer                | Transmit Multiple Deferral Frame counter.       |
| SingleCollsnFrm               | Transmit Single Collision Frame counter.        |
| MultCollsnFrm                 | Transmit Multiple Collision Frame counter.      |
| LateCollisions                | Transmit Late Collision Frame counter.          |
| ExcessivCollsns               | Transmit Excessive Collision Frame counter.     |
| Collisions                    | Transmit Total Collision counter                |
| <b>Layer 3 Counters</b>       |                                                 |
| ifInUcastPkts                 | Inbound interface Unicast counter.              |
| ifInDiscards                  | Inbound interface Discarded Packets counter.    |
| ipInHdrErrors                 | Inbound interface Header Errors counter.        |
| ifOutUcastPkts                | Outbound interface Unicast counter.             |
| ifOutErrors                   | Outbound interface Error counter.               |
| <b>Miscellaneous Counters</b> |                                                 |
| DropEvents                    | Drop Event counter                              |
| ifOutDiscards                 | Outbound interface Discarded Packets counter.   |
| MTUExcdDiscard                | Receive MTU Check Error Frame Counter           |

# speed

**Overview** This command changes the speed of the specified port. You can optionally specify the speed or speeds that get autonegotiated, so autonegotiation is only attempted at the specified speeds.

To see the currently-negotiated speed for ports whose links are up, use the [show interface](#) command. To see the configured speed (when different from the default), use the [show running-config](#) command.

**Syntax** speed {10|100|1000|auto [10][100][1000]}

The following table shows the speed options for each type of port.

| Port type                       | Speed Options (units are Mbps)      |
|---------------------------------|-------------------------------------|
| RJ-45 and RJ-5copper ports      | auto (default)<br>10<br>100<br>1000 |
| supported tri-speed copper SFPs | auto (default)<br>10<br>100<br>1000 |
| 100Mb fiber SFPs                | 100                                 |
| 1000Mb fiber SFPs               | auto (default)<br>1000              |

**Mode** Interface Configuration

**Default** By default, ports autonegotiate speed (except for 100Base-FX ports which do not support auto-negotiation, so default to 100Mbps).

**Usage** Switch ports in a static or dynamic (LACP) channel group must have the same port speed and be in full duplex mode. Once switch ports have been aggregated into a channel group, you can set the speed of all the switch ports in the channel group by applying this command to the channel group.

**NOTE:** Note that if multiple speeds are specified after the auto option to autonegotiate speeds, then only those speeds specified are attempted for autonegotiation.

**Examples** To set the speed of a tri-speed port to 100Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# speed 100
```

To return the port to auto-negotiating its speed, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# speed auto
```

To set a port to auto-negotiate its speed at 100Mbps and 1000Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# speed auto 100 1000
```

To set a port to auto-negotiate its speed at 1000Mbps only, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# speed auto 1000
```

**Related  
Commands**

[duplex](#)  
[polarity](#)  
[show interface](#)  
[speed \(asyn\)](#)

# undebbug loopprot

**Overview** This command applies the functionality of the no [debug loopprot](#) command.

# undebbug platform packet

**Overview** This command applies the functionality of the no `debug platform packet` command.

# 11

# VLAN Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure VLANs. For more information see the [VLAN Feature Overview and Configuration Guide](#).

- Command List**
- [“port-vlan-forwarding-priority”](#) on page 360
  - [“private-vlan”](#) on page 363
  - [“private-vlan association”](#) on page 364
  - [“show port-vlan-forwarding-priority”](#) on page 365
  - [“show vlan”](#) on page 366
  - [“show vlan classifier group”](#) on page 367
  - [“show vlan classifier group interface”](#) on page 368
  - [“show vlan classifier interface group”](#) on page 369
  - [“show vlan classifier rule”](#) on page 370
  - [“show vlan private-vlan”](#) on page 371
  - [“switchport access vlan”](#) on page 372
  - [“switchport enable vlan”](#) on page 373
  - [“switchport mode access”](#) on page 374
  - [“switchport mode private-vlan”](#) on page 375
  - [“switchport mode private-vlan trunk promiscuous”](#) on page 376
  - [“switchport mode private-vlan trunk secondary”](#) on page 378
  - [“switchport mode trunk”](#) on page 380
  - [“switchport private-vlan host-association”](#) on page 381
  - [“switchport private-vlan mapping”](#) on page 382

- [“switchport trunk allowed vlan”](#) on page 383
- [“switchport trunk native vlan”](#) on page 386
- [“switchport vlan-stacking \(double tagging\)”](#) on page 388
- [“switchport voice dscp”](#) on page 389
- [“switchport voice vlan”](#) on page 390
- [“switchport voice vlan priority”](#) on page 392
- [“vlan”](#) on page 393
- [“vlan classifier activate”](#) on page 394
- [“vlan classifier group”](#) on page 395
- [“vlan classifier rule ipv4”](#) on page 396
- [“vlan classifier rule proto”](#) on page 397
- [“vlan database”](#) on page 400

# port-vlan-forwarding-priority

**Overview** Use this command to set the highest priority protocol to control transitions from blocking to forwarding traffic. This command prioritizes switch port forwarding mode control, when more than one of EPSR, Loop Protection, and MAC thrashing protection protocols are used on the switch.

EPSR, Loop Protection and MAC Thrashing use the same mechanism to block or forward traffic. This command sets the highest priority protocol to control transitions from blocking to forwarding traffic. Setting the priority stops contention between protocols.

For example, If EPSR is set to the highest priority protocol to block traffic on vlan10 on port1.0.2 then this stops MAC Thrashing from forwarding traffic on vlan10 on port1.0.2.

Use the **no** variant of this command to restore the default highest priority protocol back to the default of EPSR.

For more information about EPSR, see the [EPSR Feature Overview and Configuration Guide](#).

**Syntax** `port-vlan-forwarding-priority {epsr|loop-protection|none}`  
`no port-vlan-forwarding-priority`

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| epsr            | Sets EPSR as the highest priority protocol. Use this parameter on an EPSR master node to avoid unexpected broadcast storms.                                                                                                                                                                                                                      |
| loop-protection | Sets Loop Protection as the highest priority protocol. Note that this option must not be set on an EPSR master node. Use the epsr parameter option on an EPSR master node to avoid unexpected broadcast storms.                                                                                                                                  |
| none            | Sets the protocols to have equal priority. This was the previous behavior before this command was added, and allows protocols to override each other to set a port to forwarding a VLAN. Note that this option must not be set on a EPSR master node. Use the epsr parameter option on an EPSR master node to avoid unexpected broadcast storms. |

**Default** By default, the highest priority protocol is EPSR

**Mode** Global Configuration

**Usage** EPSR, Loop Protection and MAC Thrashing protection do not usually need to be configured on a switch, because they perform similar functions—each prevents network loops by blocking a selected port for each (loop containing) VLAN.

However, if more than one of these three features is configured on a switch, you can use this command to prioritize either EPSR or Loop Protection when their effects on a port would conflict and override each other. Previously, each protocol



could set a port to forwarding for a VLAN, sometimes overriding the previous setting by another protocol to block the port. This could sometimes lead to unexpected broadcast storms.

Now, when a protocol is set to have the highest priority over a data VLAN on a port, it will not allow other protocols to put that port-vlan into a forwarding state if the highest priority protocol blocked it.

The priority mechanism is only used for blocking-to-forwarding transitions; protocols remain independent on the forwarding-to-blocking transitions.

For example, with an EPSR master node in a two-node ESPR ring with the below settings:

- The EPSR master node primary port is configured to switchport interface port1.0.1
- The EPSR master node secondary port is configured to switchport interface port1.0.2
- The EPSR master node control VLAN is configured to VLAN interface vlan10
- The EPSR master node has a first data VLAN configured to VLAN interface vlan20
- The EPSR master node has a second data VLAN configured to VLAN interface vlan30.

Initially, the EPSR ring is complete, with port1.0.2 blocking data VLANs vlan20 and vlan30 and some broadcast traffic flowing through. If the user removes vlan30 from EPSR, a storm is created on vlan30. MAC thrashing protection detects it and blocks vlan30.

Then after the storm has stopped, MAC thrashing protection sets it to forwarding again and it keeps oscillating between forwarding and blocking. In the meantime, the user adds back vlan30 to EPSR as a data VLAN and EPSR blocks it on port1.0.2.

If the priority is set to none (**port-vlan-forwarding-priority none**), MAC thrashing protection notices that the storm has stopped again and decides to put vlan30 on port1.0.2 into forwarding state. This overrides what EPSR requires for this port-VLAN and creates a storm. This matches the old behavior before this feature was implemented.

If the priority is set to EPSR or default (**port-vlan-forwarding-priority epsr**), MAC thrashing protection notices that the storm has stopped again and attempts to put vlan30 on port1.0.2 into forwarding state. The higher priority protocol (EPSR) is blocking the VLAN on this port, so it stays blocking and no storm occurs.

**Example** To prioritize EPSR over Loop Protection or MAC Thrashing protection settings, so that Loop Protection or MAC Thrashing protection cannot set a port to the forwarding state a VLAN if EPSR has set it to the blocking state, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority epsr
```

To prioritize Loop Protection over EPSR or MAC Thrashing protection settings, so that EPSR or MAC Thrashing protection cannot set a port to the forwarding state a VLAN if Loop Protection has set it to the blocking state, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority loop-protection
```

To set EPSR, Loop Protection, and MAC Thrashing protection protocols to have equal priority for port forwarding and blocking, which allows the protocols to override each other to set a port to the forwarding or blocking states, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority none
```

To restore the default highest priority protocol back to the default of EPSR, use the commands:

```
awplus# configure terminal
awplus(config)# no port-vlan-forwarding-priority
```

**Related Commands**    [show port-vlan-forwarding-priority](#)

# private-vlan

**Overview** Use this command to create a private VLAN. Private VLANs can be either primary or secondary. Secondary VLANs can be either community or isolated.

Use the **no** variant of this command to remove the specified private VLAN.

For more information, see the [VLAN Feature Overview and Configuration Guide](#).

**Syntax** `private-vlan <vlan-id> {community|isolated|primary}`  
`no private-vlan <vlan-id> {community|isolated|primary}`

| Parameter | Description                                                                                                                                                      |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <vlan-id> | VLAN ID in the range <2-4094> for the VLAN which is to be made a private VLAN.<br>VLAN ID in the range <2-2048> for the VLAN which is to be made a private VLAN. |
| community | Community VLAN.                                                                                                                                                  |
| isolated  | Isolated VLAN.                                                                                                                                                   |
| primary   | Primary VLAN.                                                                                                                                                    |

**Mode** VLAN Configuration

**Examples**

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2 name vlan2 state enable
awplus(config-vlan)# vlan 3 name vlan3 state enable
awplus(config-vlan)# vlan 4 name vlan4 state enable
awplus(config-vlan)# private-vlan 2 primary
awplus(config-vlan)# private-vlan 3 isolated
awplus(config-vlan)# private-vlan 4 community
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no private-vlan 2 primary
awplus(config-vlan)# no private-vlan 3 isolated
awplus(config-vlan)# no private-vlan 4 community
```

# private-vlan association

**Overview** Use this command to associate a secondary VLAN to a primary VLAN. Only one isolated VLAN can be associated to a primary VLAN. Multiple community VLANs can be associated to a primary VLAN.

Use the **no** variant of this command to remove association of all the secondary VLANs to a primary VLAN.

For more information, see the [VLAN Feature Overview and Configuration Guide](#).

**Syntax** `private-vlan <primary-vlan-id> association {add  
<secondary-vlan-id>|remove <secondary-vlan-id>}  
no private-vlan <primary-vlan-id> association`

| Parameter           | Description                                                   |
|---------------------|---------------------------------------------------------------|
| <primary-vlan-id>   | VLAN ID of the primary VLAN.                                  |
| <secondary-vlan-id> | VLAN ID of the secondary VLAN (either isolated or community). |

**Mode** VLAN Configuration

**Examples** The following commands associate primary VLAN 2 with secondary VLAN 3:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 2 association add 3
```

The following commands remove the association of primary VLAN 2 with secondary VLAN 3:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 2 association remove 3
```

The following commands remove all secondary VLAN associations of primary VLAN 2:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no private-vlan 2 association
```

# show port-vlan-forwarding-priority

**Overview** Use this command to display the highest priority protocol that controls port-vlan forwarding or blocking traffic. This command displays whether EPSR or Loop Protection is set as the highest priority for determining whether a port forwards a VLAN, as set by the [port-vlan-forwarding-priority](#) command.

For more information about EPSR, see the [EPSR Feature Overview and Configuration Guide](#).

**Syntax** `show port-vlan-forwarding-priority`

**Mode** Privileged Exec

**Example** To display the highest priority protocol, use the command:

```
awplus# show port-vlan-forwarding-priority
```

**Output** Figure 11-1: Example output from the **show port-vlan-forwarding-priority** command

```
Port-vlan Forwarding Priority: EPSR
```

**Related Commands** [port-vlan-forwarding-priority](#)

# show vlan

**Overview** Use this command to display information about a particular VLAN by specifying the VLAN ID. It displays information for all the VLANs configured.

**Syntax** `show vlan {all|brief|dynamic|static|auto|static-ports<1-2048>}`

| Parameter     | Description                                                  |
|---------------|--------------------------------------------------------------|
| <1-2048>      | Display information about the VLAN specified by the VLAN ID. |
| all           | Display information about all VLANs on the device.           |
| brief         | Display information about all VLANs on the device.           |
| dynamic       | Display information about all VLANs learned dynamically.     |
| static        | Display information about all statically configured VLANs.   |
| auto          | Display information about all auto-configured VLANs.         |
| static- ports | Display static egress/forbidden ports.                       |

**Mode** User Exec and Privileged Exec

**Example** To display information about VLAN 2, use the command:

```
awplus# show vlan 2
```

**Output** Figure 11-2: Example output from the **show vlan** command

| VLAN ID | Name     | Type   | State  | Member ports<br>(u)-Untagged, (t)-Tagged               |
|---------|----------|--------|--------|--------------------------------------------------------|
| 2       | VLAN0002 | STATIC | ACTIVE | port1.0.3(u) port1.0.4(u) port1.0.5(u)<br>port1.0.6(u) |
| ...     |          |        |        |                                                        |

**Related  
Commands** [vlan](#)

# show vlan classifier group

**Overview** Use this command to display information about all configured VLAN classifier groups or a specific group.

**Syntax** show vlan classifier group [<1-16>]

| Parameter | Description                      |
|-----------|----------------------------------|
| <1 - 16>  | VLAN classifier group identifier |

**Mode** User Exec and Privileged Exec

**Usage** If a group ID is not specified, all configured VLAN classifier groups are shown. If a group ID is specified, a specific configured VLAN classifier group is shown.

**Example** To display information about VLAN classifier group 1, enter the command:  
awplus# show vlan classifier group 1

**Related Commands** [vlan classifier group](#)

# show vlan classifier group interface

**Overview** Use this command to display information about a single switch port interface for all configured VLAN classifier groups.

**Syntax** show vlan classifier group interface *<switch-port>*

| Parameter                  | Description                                                   |
|----------------------------|---------------------------------------------------------------|
| <i>&lt;switch-port&gt;</i> | Specify the switch port interface classifier group identifier |

**Mode** User Exec and Privileged Exec

**Usage** All configured VLAN classifier groups are shown for a single interface.

**Example** To display VLAN classifier group information for switch port interface `port1.0.2`, enter the command:

```
awplus# show vlan classifier group interface port1.0.2
```

**Output** Figure 11-3: Example output from the **show vlan classifier group interface port1.0.1** command:

```
vlan classifier group 1 interface port1.0.1
```

**Related Commands** [vlan classifier group](#)  
[show vlan classifier interface group](#)



# show vlan classifier interface group

**Overview** Use this command to display information about all interfaces configured for a VLAN group or all the groups.

**Syntax** show vlan classifier interface group [<1-16>]

| Parameter | Description                                |
|-----------|--------------------------------------------|
| <1 - 16>  | VLAN classifier interface group identifier |

**Mode** User Exec and Privileged Exec

**Usage** If a group ID is not specified, all interfaces configured for all VLAN classifier groups are shown. If a group ID is specified, the interfaces configured for this VLAN classifier group are shown.

**Example** To display information about all interfaces configured for all VLAN groups, enter the command:

```
awplus# show vlan classifier interface group
```

To display information about all interfaces configured for VLAN group 1, enter the command:

```
awplus# show vlan classifier interface group 1
```

**Output** Figure 11-4: Example output from the **show vlan classifier interface group** command

```
vlan classifier group 1 interface port1.0.1
vlan classifier group 1 interface port1.0.2
vlan classifier group 2 interface port1.0.3
vlan classifier group 2 interface port1.0.4
```

**Output** Figure 11-5: Example output from the **show vlan classifier interface group 1** command

```
vlan classifier group 1 interface port1.0.1
vlan classifier group 1 interface port1.0.2
```

**Related Commands** [vlan classifier group](#)  
[show vlan classifier group interface](#)

# show vlan classifier rule

**Overview** Use this command to display information about all configured VLAN classifier rules or a specific rule.

**Syntax** show vlan classifier rule [<1-256>]

| Parameter | Description                     |
|-----------|---------------------------------|
| <1 - 256> | VLAN classifier rule identifier |

**Mode** User Exec and Privileged Exec

**Usage** If a rule ID is not specified, all configured VLAN classifier rules are shown. If a rule ID is specified, a specific configured VLAN classifier rule is shown.

**Example** To display information about VLAN classifier rule 1, enter the command:

```
awplus# show vlan classifier rule 1
```

**Output** Figure 11-6: Example output from the **show vlan classifier rule1** command

```
vlan classifier group 1 add rule 1
```

**Related Commands**

- [vlan classifier activate](#)
- [vlan classifier rule ipv4](#)
- [vlan classifier rule proto](#)

# show vlan private-vlan

**Overview** Use this command to display the private VLAN configuration and associations.

**Syntax** show vlan private-vlan

**Mode** User Exec and Privileged Exec

**Example** To display the private VLAN configuration and associations, enter the command:

```
awplus# show vlan private-vlan
```

**Output** Figure 11-7: Example output from the **show vlan private-vlan** command

| awplus#show vlan private-vlan |           |           |            |
|-------------------------------|-----------|-----------|------------|
| PRIMARY                       | SECONDARY | TYPE      | INTERFACES |
| -----                         | -----     | -----     | -----      |
| 2                             | 3         | isolated  |            |
| 2                             | 4         | community |            |
|                               | 8         | isolated  |            |

**Related Commands** [private-vlan](#)  
[private-vlan association](#)

# switchport access vlan

**Overview** Use this command to change the port-based VLAN of the current port.

Use the **no** variant of this command to change the port-based VLAN of this port to the default VLAN, vlan1.

**Syntax** switchport access vlan <vlan-id>  
no switchport access vlan

| Parameter | Description                                   |
|-----------|-----------------------------------------------|
| <vlan-id> | <1-2048> The port-based VLAN ID for the port. |

**Default** Reset the default VLAN 1 to specified switchports using the negated form of this command.

**Mode** Interface Configuration

**Usage** Any untagged frame received on this port will be associated with the specified VLAN.

**Examples** To change the port-based VLAN to VLAN 3 for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport access vlan 3
```

To reset the port-based VLAN to the default VLAN 1 for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport access vlan
```

**Validation Command** show interface switchport

**Related Commands** show vlan

## switchport enable vlan

**Overview** This command enables the VLAN on the port manually once disabled by certain actions, such as QSP (QoS Storm Protection) or EPSR (Ethernet Protection Switching Ring). Note that if the VID is not given, all disabled VLANs are re-enabled.

This command enables the VLAN on the port manually once disabled by certain actions, such as EPSR (Ethernet Protection Switching Ring). Note that if the VID is not given, all disabled VLANs are re-enabled.

**Syntax** switchport  
enable vlan [<1-2048>]

| Parameter | Description                      |
|-----------|----------------------------------|
| vlan      | Re-enables the VLAN on the port. |
| <1-2048>  | VLAN ID.                         |

**Mode** Interface Configuration

**Example** To re-enable the port1.0.1 from VLAN 1:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport enable vlan 1
```

# switchport mode access

**Overview** Use this command to set the switching characteristics of the port to access mode. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

**Syntax** `switchport mode access [ingress-filter {enable|disable}]`

| Parameter      | Description                                                                               |
|----------------|-------------------------------------------------------------------------------------------|
| ingress-filter | Set the ingress filtering for the received frames.                                        |
| enable         | Turn on ingress filtering for received frames. This is the default.                       |
| disable        | Turn off ingress filtering to accept frames that do not meet the classification criteria. |

**Default** By default, ports are in access mode with ingress filtering on.

**Usage** Use access mode to send untagged frames only.

**Mode** Interface Configuration

**Example**

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access ingress-filter enable
```

**Validation Command** `show interface switchport`

# switchport mode private-vlan

**Overview** Use this command to make a Layer 2 port a private VLAN host port or a promiscuous port.

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

**Syntax** `switchport mode private-vlan {host|promiscuous}`  
`no switchport mode private-vlan {host|promiscuous}`

| Parameter   | Description                                                                                                                                                                                                                                                                    |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| host        | This port type can communicate with all other host ports assigned to the same community VLAN, but it cannot communicate with the ports in the same isolated VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN. |
| promiscuous | A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN.                                                                                                                                                      |

**Mode** Interface Configuration

**Examples** `awplus# configure terminal`  
`awplus(config)# interface port1.0.2`  
`awplus(config-if)# switchport mode private-vlan host`  
`awplus(config)# interface port1.0.3`  
`awplus(config-if)# switchport mode private-vlan promiscuous`  
`awplus(config)# interface port1.0.4`  
`awplus(config-if)# no switchport mode private-vlan promiscuous`

**Related Commands** [switchport private-vlan mapping](#)

# switchport mode private-vlan trunk promiscuous

**Overview** Use this command to enable a port in trunk mode to be promiscuous port for isolated VLANs.

**NOTE:** Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. Private VLAN trunk ports and GVRP are mutually exclusive.

Use the **no** variant of this command to remove a port in trunk mode as a promiscuous port for isolated VLANs. You must first remove the secondary port, or ports, in trunk mode associated with the promiscuous port with the **no switchport mode private-vlan trunk secondary** command.

**Syntax** switchport mode private-vlan trunk promiscuous group <group-id>  
no switchport mode private-vlan trunk promiscuous

| Parameter  | Description                                                                                                               |
|------------|---------------------------------------------------------------------------------------------------------------------------|
| <group-id> | The group ID is a numeric value in the range 1 to 32 that is used to associate the promiscuous port with secondary ports. |

**Default** By default, a port in trunk mode is disabled as a promiscuous port.

**Mode** Interface Configuration

**Usage** A port must be put in trunk mode with [switchport mode trunk](#) command before it can be enabled as a promiscuous port.

To add VLANs to be trunked over the promiscuous port, use the [switchport trunk allowed vlan](#) command. These VLANs can be isolated VLANs, or non-private VLANs.

To configure the native VLAN for the promiscuous port, use the [switchport trunk native vlan](#) command. The native VLAN can be an isolated VLAN, or a non-private VLAN.

When you enable a promiscuous port, all of the secondary port VLANs associated with the promiscuous port via the group ID number must be added to the promiscuous port. In other words, the set of VLANs on the promiscuous port must be a superset of all the VLANs on the secondary ports within the group.

**Examples** To create the isolated VLANs 2, 3 and 4 and then enable port `t1.0.2` in trunk mode as a promiscuous port for these VLANs with the group ID of 3, use the following commands:



To create the isolated VLANs 2, 3 and 4 and then enable port1.1.2 in trunk mode as a promiscuous port for these VLANs with the group ID of 3, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2-4
awplus(config-vlan)# private-vlan 2 isolated
awplus(config-vlan)# private-vlan 3 isolated
awplus(config-vlan)# private-vlan 4 isolated
awplus(config-vlan)# exit
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 2-4
awplus(config-if)# switchport mode private-vlan trunk
promiscuous group 3
```

To remove port1.0.2 in trunk mode as a promiscuous port for a private VLAN, use the commands:

To remove port1.1.2 in trunk mode as a promiscuous port for a private VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport mode private-vlan trunk
promiscuous
```

Note that you must remove the secondary port or ports enabled as trunk ports that are associated with the promiscuous port before removing the promiscuous port.

**Related  
Commands**

[switchport mode private-vlan trunk secondary](#)  
[switchport mode trunk](#)  
[switchport trunk allowed vlan](#)  
[switchport trunk native vlan](#)  
[show vlan private-vlan](#)

# switchport mode private-vlan trunk secondary

**Overview** Use this command to enable a port in trunk mode to be a secondary port for isolated VLANs.

**NOTE:** Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. Private VLAN trunk ports and GVRP are mutually exclusive.

Use the **no** variant of this command to remove a port in trunk mode as a secondary port for isolated VLANs.

**Syntax** switchport mode private-vlan trunk secondary group <group-id>  
no switchport mode private-vlan trunk secondary

| Parameter  | Description                                                                                                                |
|------------|----------------------------------------------------------------------------------------------------------------------------|
| <group-id> | The group ID is a numeric value in the range 1 to 32 that is used to associate a secondary port with its promiscuous port. |

**Default** By default, a port in trunk mode is disabled as a secondary port.

When a port in trunk mode is enabled to be a secondary port for isolated VLANs, by default it will have a native VLAN of **none**(no native VLAN specified).

**Mode** Interface Configuration

**Usage** A port must be put in trunk mode with [switchport mode trunk](#) command before the port is enabled as a secondary port in trunk mode.

To add VLANs to be trunked over the secondary port use the [switchport trunk allowed vlan](#) command. These must be isolated VLANs and must exist on the associated promiscuous port.

To configure the native VLAN for the secondary port, use the [switchport trunk native vlan](#) command. The native VLAN must be an isolated VLAN and must exist on the associated promiscuous port.

**Examples** To create isolated private VLAN 2 and then enable port t1.0.3 in trunk mode as a secondary port for this VLAN with the group ID of 3, use the following commands:

To create isolated private VLAN 2 and then enable port t1.1.3 in trunk mode as a secondary port for the this VLAN with the group ID of 3, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2
awplus(config-vlan)# private-vlan 2 isolated
awplus(config-vlan)# exit
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 2
awplus(config-if)# switchport mode private-vlan trunk secondary
group 3
```

To remove port1.1.3 in trunk mode as a secondary port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no switchport mode private-vlan trunk
secondary
```

**Related  
Commands**

[switchport mode private-vlan trunk promiscuous](#)  
[switchport mode trunk](#)  
[switchport trunk allowed vlan](#)  
[switchport trunk native vlan](#)  
[show vlan private-vlan](#)

# switchport mode trunk

**Overview** Use this command to set the switching characteristics of the port to trunk. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

**Syntax** `switchport mode trunk [ingress-filter {enable|disable}]`

| Parameter      | Description                                                                               |
|----------------|-------------------------------------------------------------------------------------------|
| ingress-filter | Set the ingress filtering for the frames received.                                        |
| enable         | Turn on ingress filtering for received frames. This is the default.                       |
| disable        | Turn off ingress filtering to accept frames that do not meet the classification criteria. |

**Default** By default, ports are in access mode, are untagged members of the default VLAN (vlan1), and have ingress filtering on.

**Mode** Interface Configuration

**Usage** A port in trunk mode can be a tagged member of multiple VLANs, and an untagged member of one native VLAN.

To configure which VLANs this port will trunk for, use the [switchport trunk allowed vlan](#) command.

**Example**

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode trunk ingress-filter enable
```

**Validation Command** [show interface switchport](#)

# switchport private-vlan host-association

**Overview** Use this command to associate a primary VLAN and a secondary VLAN to a host port. Only one primary and secondary VLAN can be associated to a host port.

Use the **no** variant of this command to remove the association.

**Syntax** switchport private-vlan host-association <primary-vlan-id> add  
<secondary-vlan-id>  
no switchport private-vlan host-association

| Parameter           | Description                                                   |
|---------------------|---------------------------------------------------------------|
| <primary-vlan-id>   | VLAN ID of the primary VLAN.                                  |
| <secondary-vlan-id> | VLAN ID of the secondary VLAN (either isolated or community). |

**Mode** Interface Configuration

**Examples** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# switchport private-vlan host-association 2  
add 3  
awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# no switchport private-vlan host-association

# switchport private-vlan mapping

**Overview** Use this command to associate a primary VLAN and a set of secondary VLANs to a promiscuous port.

Use the **no** variant of this to remove all the association of secondary VLANs to primary VLANs for a promiscuous port.

**Syntax** `switchport private-vlan mapping <primary-vlan-id> add <secondary-vid-list>`  
`switchport private-vlan mapping <primary-vlan-id> remove <secondary-vid-list>`  
`no switchport private-vlan mapping`

| Parameter                               | Description                                                                                                                       |
|-----------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;primary-vlan-id&gt;</code>    | VLAN ID of the primary VLAN.                                                                                                      |
| <code>&lt;secondary-vid-list&gt;</code> | VLAN ID of the secondary VLAN (either isolated or community), or a range of VLANs, or a comma-separated list of VLANs and ranges. |

**Mode** Interface Configuration

**Usage** This command can be applied to a switch port or a static channel group, but not a dynamic (LACP) channel group. LACP channel groups (dynamic/LACP aggregators) cannot be promiscuous ports in private VLANs.

**Examples** `awplus# configure terminal`  
`awplus(config)# interface port1.0.2`  
`awplus(config-if)# switchport private-vlan mapping 2 add 3-4`  
`awplus(config-if)# switchport private-vlan mapping 2 remove 3-4`  
`awplus(config-if)# no switchport private-vlan mapping`

**Related Commands** [switchport mode private-vlan](#)

# switchport trunk allowed vlan

**Overview** Use this command to add VLANs to be trunked over this switch port. Traffic for these VLANs can be sent and received on the port.

Use the **no** variant of this command to reset switching characteristics of a specified interface to negate a trunked configuration specified with **switchport trunk allowed vlan** command.

**Syntax**

```
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add <vid-list>
switchport trunk allowed vlan remove <vid-list>
switchport trunk allowed vlan except <vid-list>
no switchport trunk
```

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all        | Allow all VLANs to transmit and receive through the port.                                                                                                                                                                                                                                                                                                                                                                                    |
| none       | Allow no VLANs to transmit and receive through the port.                                                                                                                                                                                                                                                                                                                                                                                     |
| add        | Add a VLAN to transmit and receive through the port. Only use this parameter if a list of VLANs are already configured on a port.                                                                                                                                                                                                                                                                                                            |
| remove     | Remove a VLAN from transmit and receive through the port. Only use this parameter if a list of VLANs are already configured on a port.                                                                                                                                                                                                                                                                                                       |
| except     | All VLANs, except the VLAN for which the VID is specified, are part of its port member set. Only use this parameter to remove VLANs after either this parameter or the <b>all</b> parameter have added VLANs to a port.                                                                                                                                                                                                                      |
| <vid-list> | <2-2048> The ID of the VLAN or VLANs that will be added to, or removed from, the port. A single VLAN, VLAN range, or comma-separated VLAN list can be set.<br>For a VLAN range, specify two VLAN numbers: lowest, then highest number in the range, separated by a hyphen.<br>For a VLAN list, specify the VLAN numbers separated by commas. Do not enter spaces between hyphens or commas when setting parameters for VLAN ranges or lists. |

**Default** By default, ports are untagged members of the default VLAN (vlan1).

**Mode** Interface Configuration

**Usage** The **all** parameter sets the port to be a tagged member of all the VLANs configured on the device. The **none** parameter removes all VLANs from the port's tagged member set. The **add** and **remove** parameters will add and remove VLANs to and from the port's member set. See the note below about restrictions when using the **add**, **remove**, **except**, and **all** parameters.

**NOTE:** Only use the **add** or the **remove** parameters with this command if a list of VLANs are configured on a port. Only use the **except** parameter to remove VLANs after either the **except** or the **all** parameters have first been used to add a list of VLANs to a port.

To remove a VLAN, where the configuration for port 1.0.6 shows the below output:

```
awplus#show running-config
!
interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 4
```

Remove VLAN 3 by re-entering the **except** parameter with the list of VLANs to remove, instead of using the **remove** parameter, as shown in the command example below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# switchport trunk allowed vlan except 3,4
```

Then the configuration is changed after entering the above commands to remove VLAN 3:

```
awplus#show running-config
!
interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 3-4
```

To add a VLAN, where the configuration for port 1.0.6 shows the below output:

```
awplus#show running-config
!
interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 3-5
```



Add VLAN 4 by re-entering the **except** parameter with a list of VLANs to exclude, instead of using the **add** parameter to include VLAN 4, as shown in the command example below:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport trunk allowed vlan except 3,5
```

The configuration is changed after entering the above commands to add VLAN 4:

```
awplus#show running-config

!

interface port1.0.5
switchport
switchport mode trunk
switchport trunk allowed vlan except 3,5
```

**Examples** The following shows adding a single VLAN to the port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to the port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2-4
```

The following shows adding a list of VLANs to the port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2,3,4
```

# switchport trunk native vlan

**Overview** Use this command to configure the native VLAN for this port. The native VLAN is used for classifying the incoming untagged packets. Use the **none** parameter with this command to remove the native VLAN from the port and set the acceptable frame types to vlan-tagged only.

Use the **no** variant of this command to revert the native VLAN to the default VLAN ID 1. Command negation removes tagged VLANs, and sets the native VLAN to the default VLAN.

**Syntax** switchport trunk native vlan {<vid>|none}  
no switchport trunk native vlan

| Parameter | Description                                                                                                                                                                                                                                                                                        |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <vid>     | <2 - 2048><br>The ID of the VLAN that will be used to classify the incoming untagged packets. The VLAN ID must be a part of the VLAN member set of the port.                                                                                                                                       |
| none      | No native VLAN specified. This option removes the native VLAN from the port and sets the acceptable frame types to vlan-tagged only. Note: Use the <b>no</b> variant of this command to revert to the default VLAN 1 as the native VLAN for the specified interface switchport - not <b>none</b> . |

**Default** VLAN 1 (the default VLAN), which is reverted to using the **no** form of this command.

**Mode** Interface Configuration

**Examples** The following commands show configuration of VLAN 2 as the native VLAN for interface port1.0.2:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk native vlan 2
```

The following commands show the removal of the native VLAN for interface port1.0.2:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk native vlan none
```

The following commands revert the native VLAN to the default VLAN 1 for interface port1.0.2:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport trunk native vlan
```

# switchport vlan-stacking (double tagging)

**Overview** Use this command to enable VLAN stacking on a port and set it to be a customer-edge-port or provider-port. This is sometimes referred to as VLAN double-tagging, nested VLANs, or Q in Q.

Use **no** parameter with this command to disable VLAN stacking on an interface.

**Syntax** switchport vlan-stacking {customer-edge-port|provider-port}  
no switchport vlan-stacking

| Parameter          | Description                                                                        |
|--------------------|------------------------------------------------------------------------------------|
| customer-edge-port | Set the port to be a customer edge port. This port must already be in access mode. |
| provider-port      | Set the port to be a provider port. This port must already be in trunk mode.       |

**Default** By default, ports are not VLAN stacking ports.

**Mode** Interface Configuration

**Usage** Use VLAN stacking to separate traffic from different customers so that they can be managed over a provider network.  
Traffic with an extra VLAN header added by VLAN stacking cannot be routed.

**Example** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# switchport vlan-stacking customer-edge-port

# switchport voice dscp

**Overview** Use this command to configure the Layer 3 DSCP value advertised when the transmission of LLDP-MED Network Policy TLVs for voice devices is enabled. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified DSCP value.

Use the **no** variant of this command to reset the DSCP value to the default, 0.

**Syntax** `switchport voice dscp <0-63>`  
`no switchport voice dscp`

| Parameter | Description                          |
|-----------|--------------------------------------|
| dscp      | Specify a DSCP value for voice data. |
| <0-63>    | DSCP value.                          |

**Default** A DSCP value of 0 will be advertised.

**Mode** Interface Configuration

**Usage** LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled ([lldp run](#) command)
- Voice VLAN is configured for the port ([switchport voice vlan](#) command)
- The port is configured to transmit LLDP advertisements—enabled by default ([lldp transmit receive](#) command)
- The port is configured to transmit Network Policy TLVs—enabled by default ([lldp med-tlv-select](#) command)
- There is an LLDP-MED device connected to the port

**Example** To tell IP phones connected to port 1.0.5 to send voice data with DSCP value 27, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport voice dscp 27
```

**Related Commands** [lldp med-tlv-select](#)  
[show lldp](#)  
[switchport voice vlan](#)

# switchport voice vlan

**Overview** Use this command to configure the Voice VLAN tagging advertised when the transmission of LLDP-MED Network Policy TLVs for voice endpoint devices is enabled. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified tagging. This command also sets the ports to be spanning tree edge ports, that is, it enables spanning tree portfast on the ports.

Use the **no** variant of this command to remove LLDP-MED network policy configuration for voice devices connected to these ports. This does not change the spanning tree edge port status.

**Syntax** `switchport voice vlan [<vid>|dot1p|dynamic|untagged]`  
`no switchport voice vlan`

| Parameter | Description                                                                                                                                                                                                                                   |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <vid>     | VLAN identifier, in the range 1 to 2048.                                                                                                                                                                                                      |
| dot1p     | The IP phone should send User Priority tagged packets, that is, packets in which the tag contains a User Priority value, and a VID of 0. (The User Priority tag is also known as the 802.1p priority tag, or the Class of Service (CoS) tag.) |
| dynamic   | The VLAN ID with which the IP phone should send tagged packets will be assigned by RADIUS authentication.                                                                                                                                     |
| untagged  | The IP phone should send untagged packets.                                                                                                                                                                                                    |

**Default** By default, no Voice VLAN is configured, and therefore no network policy is advertised for voice devices.

**Mode** Interface Configuration

**Usage** LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled ([lldp run](#) command)
- Voice VLAN is configured for the port using this command ([switchport voice vlan](#))
- The port is configured to transmit LLDP advertisements—enabled by default ([lldp transmit receive](#) command)
- The port is configured to transmit Network Policy TLVs—enabled by default ([lldp med-tlv-select](#) command)
- There is an LLDP-MED device connected to the port.

To set the priority value to be advertised for tagged frames, use the [switchport voice vlan priority](#) command.

If the Voice VLAN details are to be assigned by RADIUS, then the RADIUS server must be configured to send the attribute "Egress-VLANID (56)" or "Egress-VLAN-Name (58)" in the RADIUS Accept message when authenticating a phone attached to this port.

For more information about configuring authentication for Voice VLAN, see the [LLDP Feature Overview and Configuration Guide](#).

If the ports have been set to be edge ports by the [switchport voice vlan](#) command, the **no** variant of this command will leave them unchanged as edge ports. To set them back to their default non-edge port configuration, use the [spanning-tree edgeport \(RSTP and MSTP\)](#) command.

**Examples** To tell IP phones connected to port 1.0.5 to send voice data tagged for VLAN 10, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport voice vlan 10
```

To tell IP phones connected to ports 1.0.2-1.0.6 to send priority tagged packets (802.1p priority tagged with VID 0, so that they will be assigned to the port VLAN) use the following commands. The priority value is 5 by default, but can be configured with the [switchport voice vlan priority](#) command.

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.6
awplus(config-if)# switchport voice vlan dot1p
```

To dynamically configure the VLAN ID advertised to IP phones connected to port 1.0.1 based on the VLAN assigned by RADIUS authentication (with RADIUS attribute "Egress-VLANID" or "Egress-VLAN-Name" in the RADIUS accept packet), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport voice vlan dynamic
```

To remove the Voice VLAN, and therefore disable the transmission of LLDP-MED network policy information for voice devices on port 1.0.6, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no switchport voice vlan
```

# switchport voice vlan priority

**Overview** Use this command to configure the Layer 2 user priority advertised when the transmission of LLDP-MED Network Policy TLVs for voice devices is enabled. This is the priority in the User Priority field of the IEEE 802.1Q VLAN tag, also known as the Class of Service (CoS), or 802.1p priority. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified priority.

**Syntax** `switchport voice vlan priority <0-7>`  
`no switchport voice vlan priority`

| Parameter                | Description                                   |
|--------------------------|-----------------------------------------------|
| <code>priority</code>    | Specify a user priority value for voice data. |
| <code>&lt;0-7&gt;</code> | Priority value.                               |

**Default** By default, the Voice VLAN user priority value is 5.

**Mode** Interface Configuration

**Usage** LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (`lldp run` command)
- Voice VLAN is configured for the port (`switchport voice vlan` command)
- The port is configured to transmit LLDP advertisements—enabled by default (`lldp transmit receive` command)
- The port is configured to transmit Network Policy TLVs—enabled by default (`lldp med-tlv-select` command)
- There is an LLDP-MED device connected to the port.

To set the Voice VLAN tagging to be advertised, use the `switchport voice vlan` command.

**Example** To remove the Voice VLAN, and therefore disable the transmission of LLDP-MED network policy information for voice devices on port 1.0.6, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no switchport voice vlan
```

**Related Commands** `lldp med-tlv-select`  
`show lldp`  
`switchport voice vlan`



# vlan

**Overview** This command creates VLANs, assigns names to them, and enables or disables them. Specifying the `disable` state causes all forwarding over the specified VLAN ID to cease. Specifying the `enable` state allows forwarding of frames on the specified VLAN.

The **no** variant of this command destroys the specified VLANs.

**Syntax** `vlan <vid> [name <vlan-name>] [state {enable|disable}]`  
`vlan <vid-range> [state {enable|disable}]`  
`vlan {<vid>|<vlan-name>} [mtu <mtu-value>]`  
`no vlan {<vid>|<vid-range>} [mtu]`

| Parameter   | Description                                                                                               |
|-------------|-----------------------------------------------------------------------------------------------------------|
| <vid>       | The VID of the VLAN to enable or disable in the range < 1-2048>.                                          |
| <vlan-name> | The ASCII name of the VLAN. Maximum length: <b>32</b> characters.                                         |
| <vid-range> | Specifies a range of VLAN identifiers.                                                                    |
| <mtu-value> | Specifies the Maximum Transmission Unit (MTU) size in bytes, in the range 68 to 1500 bytes, for the VLAN. |
| enable      | Sets VLAN into an <code>enable</code> state.                                                              |
| disable     | Sets VLAN into a <code>disable</code> state.                                                              |

**Default** By default, VLANs are enabled when they are created.

**Mode** VLAN Configuration

**Examples** `awplus# configure terminal`  
`awplus(config)# vlan database`  
`awplus(config-vlan)# vlan 45 name accounts state enable`  
`awplus# configure terminal`  
`awplus(config)# vlan database`  
`awplus(config-vlan)# no vlan 45`

**Related Commands** [mtu](#)  
[vlan database](#)  
[show vlan](#)

# vlan classifier activate

**Overview** Use this command in Interface Configuration mode to associate a VLAN classifier group with the switch port.

Use the **no** variant of this command to remove the VLAN classifier group from the switch port.

**Syntax** `vlan classifier activate <vlan-class-group-id>`  
`no vlan classifier activate <vlan-class-group-id>`

| Parameter                                | Description                                                     |
|------------------------------------------|-----------------------------------------------------------------|
| <code>&lt;vlan-class-group-id&gt;</code> | Specify a VLAN classifier group identifier in the range <1-16>. |

**Mode** Interface Configuration mode for a switch port.

**Usage** See the protocol-based VLAN configuration example in the [VLAN Feature Overview and Configuration Guide](#) for configuration details.

**Example** To associate VLAN classifier group 3 with switch port `1.0.3`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# vlan classifier activate 3
```

To remove VLAN classifier group 3 from switch port `1.0.3`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no vlan classifier activate 3
```

**Related Commands**

- [show vlan classifier rule](#)
- [vlan classifier group](#)
- [vlan classifier rule ipv4](#)
- [vlan classifier rule proto](#)

# vlan classifier group

**Overview** Use this command to create a group of VLAN classifier rules. The rules must already have been created.

Use the **no** variant of this command to delete a group of VLAN classifier rules.

**Syntax** `vlan classifier group <1-16> {add|delete} rule  
<vlan-class-rule-id>  
no vlan classifier group <1-16>`

| Parameter            | Description                          |
|----------------------|--------------------------------------|
| <1-16>               | VLAN classifier group identifier     |
| add                  | Add the rule to the group.           |
| delete               | Delete the rule from the group.      |
| <vlan-class-rule-id> | The VLAN classifier rule identifier. |

**Mode** Global Configuration

**Example** `awplus# configure terminal  
awplus(config)# vlan classifier group 3 add rule 5`

**Related  
Commands** [show vlan classifier rule](#)  
[vlan classifier activate](#)  
[vlan classifier rule ipv4](#)  
[vlan classifier rule proto](#)

## vlan classifier rule ipv4

**Overview** Use this command to create an IPv4 subnet-based VLAN classifier rule and map it to a specific VLAN. Use the **no** variant of this command to delete the VLAN classifier rule.

**Syntax** `vlan classifier rule <1-256> ipv4 <ip-addr/prefix-length> vlan <1-2048>`  
`no vlan classifier rule <1-256>`

| Parameter               | Description                                                                    |
|-------------------------|--------------------------------------------------------------------------------|
| <1-256>                 | Specify the VLAN Classifier Rule identifier.                                   |
| <ip-addr/prefix-length> | Specify the IP address and prefix length.                                      |
| <1-2048>                | Specify a VLAN ID to which an untagged packet is mapped in the range <1-2048>. |

**Mode** Global Configuration

**Usage** If the source IP address matches the IP subnet specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN.

**Example** `awplus# configure`  
`terminal`  
`awplus(config)# vlan`  
`classifier rule 3 ipv4 3.3.3.3/8 vlan 5`

**Related Commands** [show vlan classifier rule](#)  
[vlan classifier activate](#)  
[vlan classifier rule proto](#)

## vlan classifier rule proto

**Overview** Use this command to create a protocol type-based VLAN classifier rule, and map it to a specific VLAN. See the published IANA EtherType IEEE 802 numbers here:

[www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt](http://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt).

Instead of a protocol name the decimal value of the protocol's EtherType can be entered. The EtherType field is a two-octet field in an Ethernet frame. It is used to show which protocol is encapsulated in the payload of the Ethernet frame. Note that EtherTypes in the IANA 802 numbers are given as hexadecimal values.

The **no** variant of this command removes a previously set rule.

**Syntax** `vlan classifier rule <1-256> proto <protocol> encap ethv2 vlan <1-2048>`

`no vlan classifier rule <1-256>`

| Parameter                       | Description                                                                                          |
|---------------------------------|------------------------------------------------------------------------------------------------------|
| <1 - 256>                       | VLAN Classifier identifier                                                                           |
| proto                           | Protocol type                                                                                        |
| <protocol>                      | Specify a protocol either by its decimal number (0-65535) or by one of the following protocol names: |
| [ arp   2054 ]                  | Address Resolution protocol                                                                          |
| [ atalkarp   33011 ]            | Appletalk AARP protocol                                                                              |
| [ atalkddp   32923 ]            | Appletalk DDP protocol                                                                               |
| [ atmmulti   34892 ]            | MultiProtocol Over ATM protocol                                                                      |
| [ atmtransport   34948 ]        | Frame-based ATM Transport protocol                                                                   |
| [ dec   24576 ]                 | DEC Assigned protocol                                                                                |
| [ deccustom   24582 ]           | DEC Customer use protocol                                                                            |
| [ decdiagnostics   24581 ]      | DEC Systems Comms Arch protocol                                                                      |
| [ decdnadumpload   24577 ]      | DEC DNA Dump/Load protocol                                                                           |
| [ decdnareMOTEconsole   24578 ] | DEC DNA Remote Console protocol                                                                      |
| [ decdnarouting   24579 ]       | DEC DNA Routing protocol                                                                             |

| Parameter              | Description                                                                   |
|------------------------|-------------------------------------------------------------------------------|
| [declat   24580]       | DEC LAT protocol                                                              |
| [decsyscomm   24583]   | DEC Systems Comms Arch protocol                                               |
| [g8bpqx25   2303]      | G8BPQ AX.25 protocol                                                          |
| [ieeeaddrtrans   2561] | Xerox IEEE802.3 PUP Address                                                   |
| [ieeepup   2560]       | Xerox IEEE802.3 PUP protocol                                                  |
| [ip   2048]            | IP protocol                                                                   |
| [ipv6   34525]         | IPv6 protocol                                                                 |
| [ipx   33079]          | IPX protocol                                                                  |
| [netbeui   61680]      | IBM NETBIOS/NETBEUI protocol                                                  |
| [netbeui   61681]      | IBM NETBIOS/NETBEUI protocol                                                  |
| [pppdiscovery   34915] | PPPoE discovery protocol                                                      |
| [pppsession   34916]   | PPPoE session protocol                                                        |
| [rarp   32821]         | Reverse Address Resolution protocol                                           |
| [x25   2056]           | CCITT.25 protocol                                                             |
| [xeroxaddrtrans   513] | Xerox PUP Address Translation protocol                                        |
| [xeroxpup   512]       | Xerox PUP protocol                                                            |
| ethv2                  | Ethernet Version 2 encapsulation                                              |
| <1 - 4094>             | Specify a VLAN ID to which an untagged packet is mapped in the range <1-4094> |
| <1 - 2048>             | Specify a VLAN ID to which an untagged packet is mapped in the range <1-2048> |

**Mode** Global Configuration

**Usage** If the protocol type matches the protocol specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN. Ethernet Frame Numbers may be entered in place of the protocol names listed. For a full list please refer to the IANA list  
online:[www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt](http://www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt)

**Examples**    `awplus# configure terminal`  
`awplus(config)# vlan classifier rule 1 proto x25 encaps ethv2`  
`vlan 2`  
`awplus(config)# vlan classifier rule 2 proto 512 encaps ethv2`  
`vlan 2`  
`awplus(config)# vlan classifier rule 3 proto 2056 encaps ethv2`  
`vlan 2`  
`awplus(config)# vlan classifier rule 4 proto 2054 encaps ethv2`  
`vlan 2`  
`awplus(config)# vlan classifier rule 5 proto    encaps ethv2 vlan`  
`234525`  
`awplus(config)# vlan classifier rule 6 proto    encaps ethv2 vlan`  
`2ipv6`  
`awplus(config)# vlan classifier rule 7 proto    encaps ethv2 vlan`  
`22048`  
`awplus(config)# vlan classifier rule 8 proto    encaps ethv2 vlan`  
`2ip`

**Validation**    `awplus# show vlan classifier rule`  
**Output**

```
vlan classifier rule 16 proto rarp encaps ethv2 vlan 2
vlan classifier rule 8 proto encaps ethv2 vlan 2
vlan classifier rule 4 proto arp encaps ethv2 vlan 2
vlan classifier rule 3 proto xeroxpup encaps ethv2 vlan 2
vlan classifier rule 2 proto ip encaps ethv2 vlan 2
vlan classifier rule 1 proto ipv6 encaps ethv2 vlan 2
```

**Related**    [show vlan classifier rule](#)  
**Commands**    [vlan classifier activate](#)  
                  [vlan classifier group](#)

# vlan database

**Overview** Use this command to enter the VLAN Configuration mode.

**Syntax** `vlan database`

**Mode** Global Configuration

**Usage** Use this command to enter the VLAN configuration mode. You can then add or delete a VLAN, or modify its values.

**Example** In the following example, note the change to VLAN configuration mode from Configure mode:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)#
```

**Related  
Commands** [vlan](#)



# 12

# Spanning Tree Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure RSTP, STP or MSTP. For information about spanning trees, including configuration procedures, see the [STP Feature Overview and Configuration Guide](#).

- Command List**
- “clear spanning-tree statistics” on page 403
  - “clear spanning-tree detected protocols (RSTP and MSTP)” on page 404
  - “debug mstp (RSTP and STP)” on page 405
  - “instance priority (MSTP)” on page 409
  - “instance vlan (MSTP)” on page 411
  - “region (MSTP)” on page 413
  - “revision (MSTP)” on page 414
  - “show debugging mstp” on page 415
  - “show spanning-tree” on page 416
  - “show spanning-tree brief” on page 419
  - “show spanning-tree mst” on page 420
  - “show spanning-tree mst config” on page 421
  - “show spanning-tree mst detail” on page 422
  - “show spanning-tree mst detail interface” on page 424
  - “show spanning-tree mst instance” on page 426
  - “show spanning-tree mst instance interface” on page 427
  - “show spanning-tree mst interface” on page 428
  - “show spanning-tree mst detail interface” on page 429
  - “show spanning-tree statistics” on page 431

- ["show spanning-tree statistics instance"](#) on page 433
- ["show spanning-tree statistics instance interface"](#) on page 435
- ["show spanning-tree statistics interface"](#) on page 437
- ["show spanning-tree vlan range-index"](#) on page 440
- ["spanning-tree autoedge \(RSTP and MSTP\)"](#) on page 441
- ["spanning-tree bpdu"](#) on page 442
- ["spanning-tree cisco-interoperability \(MSTP\)"](#) on page 444
- ["spanning-tree edgeport \(RSTP and MSTP\)"](#) on page 445
- ["spanning-tree enable"](#) on page 446
- ["spanning-tree errdisable-timeout enable"](#) on page 448
- ["spanning-tree errdisable-timeout interval"](#) on page 449
- ["spanning-tree force-version"](#) on page 450
- ["spanning-tree forward-time"](#) on page 451
- ["spanning-tree guard root"](#) on page 452
- ["spanning-tree hello-time"](#) on page 453
- ["spanning-tree link-type"](#) on page 454
- ["spanning-tree max-age"](#) on page 455
- ["spanning-tree max-hops \(MSTP\)"](#) on page 456
- ["spanning-tree mode"](#) on page 457
- ["spanning-tree mst configuration"](#) on page 458
- ["spanning-tree mst instance"](#) on page 459
- ["spanning-tree mst instance path-cost"](#) on page 460
- ["spanning-tree mst instance priority"](#) on page 462
- ["spanning-tree mst instance restricted-role"](#) on page 463
- ["spanning-tree mst instance restricted-tcn"](#) on page 464
- ["spanning-tree path-cost"](#) on page 466
- ["spanning-tree portfast \(STP\)"](#) on page 467
- ["spanning-tree portfast bpdu-filter"](#) on page 469
- ["spanning-tree portfast bpdu-guard"](#) on page 471
- ["spanning-tree priority \(bridge priority\)"](#) on page 473
- ["spanning-tree priority \(port priority\)"](#) on page 474
- ["spanning-tree restricted-role"](#) on page 475
- ["spanning-tree restricted-tcn"](#) on page 476
- ["spanning-tree transmit-holdcount"](#) on page 477
- ["undebg mstp"](#) on page 478

# clear spanning-tree statistics

**Overview** Use this command to clear all the STP BPDU (Bridge Protocol Data Unit) statistics.

**Syntax** `clear spanning-tree statistics`  
`clear spanning-tree statistics [instance <mstp-instance>]`  
`clear spanning-tree statistics [interface <port> [instance <mstp-instance>]]`

| Parameter       | Description                                                                                                                                                                 |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <port>          | The port to clear STP BPDU statistics for. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |
| <mstp-instance> | The MSTP instance (MSTI - Multiple Spanning Tree Instance) to clear MSTP BPDU statistics.                                                                                   |

**Mode** User Exec and Privileged Exec

**Usage** Use this command with the **instance** parameter in MSTP mode. Specifying this command with the **interface** parameter only not the instance parameter will work in STP and RSTP mode.

**Examples** `awplus# clear spanning-tree statistics`  
`awplus# clear spanning-tree statistics instance 1`  
`awplus# clear spanning-tree statistics interface port1.0.2`  
`awplus# clear spanning-tree statistics interface port1.0.2 instance 1`

# clear spanning-tree detected protocols (RSTP and MSTP)

**Overview** Use this command to clear the detected protocols for a specific port, or all ports.  
Use this command in RSTP or MSTP mode only.

**Syntax** `clear spanning-tree detected protocols [interface <port>]`

| Parameter | Description                                                                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <port>    | The port to clear detected protocols for. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |

**Mode** Privileged Exec

**Example** `awplus# clear spanning-tree detected protocols`

## debug mstp (RSTP and STP)

**Overview** Use this command to enable debugging for the configured spanning tree mode, and echo data to the console, at various levels. Note that although this command uses the keyword **mstp** it displays debugging output for RSTP and STP protocols as well the MSTP protocol.

Use the **no** variant of this command to disable spanning tree debugging.

**Syntax**

```
debug mstp {all|cli|protocol [detail]|timer [detail]}
debug mstp {packet {rx|tx} [decode] [interface <interface>]}
debug mstp {topology-change [interface <interface>]}
no debug mstp {all|cli|protocol [detail]|timer [detail]}
no debug mstp {packet {rx|tx} [decode] [interface <interface>]}
no debug mstp {topology-change [interface <interface>]}
```

| Parameter       | Description                                                             |
|-----------------|-------------------------------------------------------------------------|
| all             | Echoes all spanning tree debugging levels to the console.               |
| cli             | Echoes spanning tree commands to the console.                           |
| packet          | Echoes spanning tree packets to the console.                            |
| rx              | Received packets.                                                       |
| tx              | Transmitted packets.                                                    |
| protocol        | Echoes protocol changes to the console.                                 |
| timer           | Echoes timer information to the console.                                |
| detail          | Detailed output.                                                        |
| decode          | Interprets packet contents                                              |
| topology-change | Interprets topology change messages                                     |
| interface       | Keyword before <interface> placeholder to specify an interface to debug |
| <interface>     | Placeholder used to specify the name of the interface to debug.         |

**Mode** Privileged Exec and Global Configuration mode

**Usage 1** Use the **debug mstp topology-change interface** command to generate debugging messages when the device receives an indication of a topology change in a BPDU from another device. The debugging can be activated on a per-port basis. Although this command uses the keyword **mstp**, it displays debugging output for RSTP and STP protocols as well as the MSTP protocol.

Due to the likely volume of output, these debug messages are best viewed using the [terminal monitor](#) command before issuing the relevant **debug mstp**

command. The default terminal monitor filter will select and display these messages. Alternatively, the messages can be directed to any of the other log outputs by adding a filter for the MSTP application using [log buffered \(filter\)](#) command:

```
awplus# configure terminal
awplus(config)# log buffered program mstp
```

### Output 1

```
awplus#terminal monitor
awplus#debug mstp topology-change interface port1.0.4
10:09:09 awplus MSTP[1409]: Topology change rcvd on port1.0.4 (internal)
10:09:09 awplus MSTP[1409]: Topology change rcvd on MSTI 1 port1.0.4
aawplus#debug mstp topology-change interface port1.0.6
10:09:29 awplus MSTP[1409]: Topology change rcvd on port1.0.6 (external)
10:09:29 awplus MSTP[1409]: Topology change rcvd on MSTI 1 port1.0.6
```

**Usage 2** Use the **debug mstp packet rx|tx decode interface** command to generate debugging messages containing the entire contents of a BPDU displayed in readable text for transmitted and received xSTP BPDUs. The debugging can be activated on a per-port basis and transmit and receive debugging is controlled independently. Although this command uses the keyword **mstp**, it displays debugging output for RSTP and STP protocols as well as the MSTP protocol.

Due to the likely volume of output, these debug messages are best viewed using the [terminal monitor](#) command before issuing the relevant **debug mstp** command. The default terminal monitor filter will select and display these messages. Alternatively, the messages can be directed to any of the other log outputs by adding a filter for the MSTP application using the [log buffered \(filter\)](#) command:

```
awplus(config)# log buffered program mstp
```

**Output 2** In MSTP mode - an MSTP BPDU with 1 MSTI:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
17:23:42 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:23:42 awplus MSTP[1417]: Protocol version: MSTP, BPDU type: RST
17:23:42 awplus MSTP[1417]: CIST Flags: Agree Forward Learn role=Desig
17:23:42 awplus MSTP[1417]: CIST root id : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST ext pathcost : 0
17:23:42 awplus MSTP[1417]: CIST reg root id : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST port id : 8001 (128:1)
17:23:42 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:23:42 awplus MSTP[1417]: Version 3 length : 80
17:23:42 awplus MSTP[1417]: Format id : 0
17:23:42 awplus MSTP[1417]: Config name : test
17:23:42 awplus MSTP[1417]: Revision level : 0
17:23:42 awplus MSTP[1417]: Config digest : 3ab68794d602fdf43b21c0b37ac3bca8
17:23:42 awplus MSTP[1417]: CIST int pathcost : 0
17:23:42 awplus MSTP[1417]: CIST bridge id : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST hops remaining : 20
17:23:42 awplus MSTP[1417]: MSTI flags : Agree Forward Learn role=Desig
17:23:42 awplus MSTP[1417]: MSTI reg root id : 8001:0000cd1000fe
17:23:42 awplus MSTP[1417]: MSTI pathcost : 0
17:23:42 awplus MSTP[1417]: MSTI bridge priority : 32768 port priority : 128
17:23:42 awplus MSTP[1417]: MSTI hops remaining : 20
17:23:42 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - finish
```

In STP mode transmitting a TCN BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet tx decode interface port1.0.4
17:28:09 awplus MSTP[1417]: port1.0.4 xSTP BPDU tx - start
17:28:09 awplus MSTP[1417]: Protocol version: STP, BPDU type: TCN
17:28:09 awplus MSTP[1417]: port1.0.4 xSTP BPDU tx - finish
```

In STP mode receiving an STP BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
17:31:36 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:31:36 awplus MSTP[1417]: Protocol version: STP, BPDU type: Config
17:31:36 awplus MSTP[1417]: Flags: role=none
17:31:36 awplus MSTP[1417]: Root id : 8000:0000cd1000fe
17:31:36 awplus MSTP[1417]: Root pathcost : 0
17:31:36 awplus MSTP[1417]: Bridge id : 8000:0000cd1000fe
17:31:36 awplus MSTP[1417]: Port id : 8001 (128:1)
17:31:36 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:31:36 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - finish
```

In RSTP mode receiving an RSTP BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
awplus#17:30:17 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:30:17 awplus MSTP[1417]: Protocol version: RSTP, BPDU type: RST
17:30:17 awplus MSTP[1417]: CIST Flags: Forward Learn role=Desig
17:30:17 awplus MSTP[1417]: CIST root id : 8000:0000cd1000fe
17:30:17 awplus MSTP[1417]: CIST ext pathcost : 0
17:30:17 awplus MSTP[1417]: CIST reg root id : 8000:0000cd1000fe
17:30:17 awplus MSTP[1417]: CIST port id : 8001 (128:1)
17:30:17 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:30:17 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - finish
```

**Examples**

```
awplus# debug mstp all
awplus# debug mstp cli
awplus# debug mstp packet rx
awplus# debug mstp protocol detail
awplus# debug mstp timer
awplus# debug mstp packet rx decode interface port1.0.2
awplus# debug mstp packet tx decode interface port1.0.6
```

**Related Commands**

- [log buffered \(filter\)](#)
- [show debugging mstp](#)
- [terminal monitor](#)
- [undebg mstp](#)



# instance priority (MSTP)

**Overview** Use this command to set the priority for this device to become the root bridge for the specified MSTI (Multiple Spanning Tree Instance).

Use this command for MSTP only.

Use the **no** variant of this command to restore the root bridge priority of the device for the instance to the default.

**Syntax** `instance <msti-id> priority <priority>`  
`no instance <msti-id> priority`

| Parameter                     | Description                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;msti-id&gt;</code>  | Specify the The MST instance ID in the range <1-15>.                                                                                                                                                                                                                                                                                                                     |
| <code>&lt;priority&gt;</code> | Specify the root bridge priority for the device for the MSTI in the range <0-61440>. Note that a lower priority number indicates a greater likelihood of the device becoming the root bridge. The priority values can be set only in increments of 4096. If you specify a number that is not a multiple of 4096, it will be rounded down. The default priority is 32768. |

**Default** The default priority value for all instances is 32768.

**Mode** MST Configuration

**Usage** MSTP lets you distribute traffic more efficiently across a network by blocking different links for different VLANs. You do this by making different devices into the root bridge for each MSTP instance, so that each instance blocks a different link.

If all devices have the same root bridge priority for the instance, MSTP selects the device with the lowest MAC address to be the root bridge. Give the device a higher priority for becoming the root bridge for a particular instance by assigning it a lower priority number, or vice versa.

**Examples** To set the root bridge priority for MSTP instance 2 to be the highest (0), so that it will be the root bridge for this instance when available, use the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 2 priority 0
```

To reset the root bridge priority for instance 2 to the default (32768), use the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# no instance 2 priority
```

**Related  
Commands**

- region (MSTP)
- revision (MSTP)
- show spanning-tree mst config
- spanning-tree mst instance
- spanning-tree mst instance priority

# instance vlan (MSTP)

**Overview** Use this command to create an MST Instance (MSTI), and associate the specified VLANs with it. An MSTI is a spanning tree instance that exists within an MST region (MSTR). An MSTR can contain up to 15 MSTIs.

When a VLAN is associated with an MSTI the member ports of the VLAN are automatically configured to send and receive spanning-tree information for the associated MSTI. You can disable this automatic configuration of member ports of the VLAN to the associated MSTI by using a **no spanning-tree mst instance** command to remove the member port from the MSTI.

Use the **instance vlan** command for MSTP only.

Use the **no** variant of this command to remove the specified VLANs from the MSTI.

**Syntax** `instance <msti-id> vlan {<vid>|<vid-list>}`  
`no instance <msti-id> vlan {<vid>|<vid-list>}`

| Parameter  | Description                                                                                       |
|------------|---------------------------------------------------------------------------------------------------|
| <msti-id>  | Specify the MST instance ID <1 - 15>.                                                             |
| <vid>      | Specify a VLAN identifier (VID) in the range <1 - 4094> to be associated with the MSTI specified. |
| <vid-list> | A hyphen-separated range or a comma-separated list of VLAN IDs                                    |

**Mode** MST Configuration

**Usage** The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

This command removes the specified VLANs from the CIST and adds them to the specified MSTI. If you use the **no** variant of this command to remove the VLAN from the MSTI, it returns it to the CIST. To move a VLAN from one MSTI to another, you must first use the **no** variant of this command to return it to the CIST.

Ports in these VLANs will remain in the control of the CIST until you associate the ports with the MSTI using the [spanning-tree mst instance](#) command.

**Example** `awplus# configure terminal`  
`awplus(config)# spanning-tree mode mstp`  
`awplus(config)# spanning-tree mst configuration`  
`awplus(config-mst)# instance 2 vlan 30`

**Related  
Commands**

- region (MSTP)
- revision (MSTP)
- show spanning-tree mst config
- spanning-tree mst instance
- vlan

## region (MSTP)

**Overview** Use this command to assign a name to the device's MST Region. MST Instances (MSTI) of a region form different spanning trees for different VLANs.

Use this command for MSTP only.

Use the **no** variant of this command to remove this region name and reset it to the default.

**Syntax** `region <region-name>`  
`no region`

| Parameter                        | Description                                                                                                           |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| <code>&lt;region-name&gt;</code> | Specify the name of the region, up to 32 characters. Valid characters are upper-case, lower-case, digits, underscore. |

**Default** By default, the region name is My Name.

**Mode** MST Configuration

**Usage** The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

**Example** `awplus# configure terminal`  
`awplus(config)# spanning-tree mst configuration`  
`awplus(config-mst)# region ATL`

**Related Commands** [revision \(MSTP\)](#)  
[show spanning-tree mst config](#)

## revision (MSTP)

**Overview** Use this command to specify the MST revision number to be used in the configuration identifier.

Use this command for MSTP only.

**Syntax** `revision <revision-number>`

| Parameter                            | Description                                   |
|--------------------------------------|-----------------------------------------------|
| <code>&lt;revision-number&gt;</code> | <code>&lt;0-65535&gt;</code> Revision number. |

**Default** The default of revision number is 0.

**Mode** MST Configuration

**Usage** The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

**Example**

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# revision 25
```

**Related Commands**

- [region \(MSTP\)](#)
- [show spanning-tree mst config](#)
- [instance vlan \(MSTP\)](#)

# show debugging mstp

**Overview** Use this command to show the MSTP debugging options set.

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 debugging mstp

**Mode** User Exec and Privileged Exec mode

**Example** To display the MSTP debugging options set, enter the command:

```
awplus# show debugging mstp
```

**Output** Figure 12-1: Example output from the **show debugging mstp** command

```
MSTP debugging status:
MSTP receiving packet debugging is on
```

**Related Commands** [debug mstp \(RSTP and STP\)](#)

# show spanning-tree

**Overview** Use this command to display detailed spanning tree information on the specified port or on all ports. Use this command for RSTP, MSTP or STP.

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 spanning-tree [interface <port-list>]

| Parameter   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface   | Display information about the following port only.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <port-list> | The ports to display information about. A port-list can be: <ul style="list-style-type: none"><li>• a switch port (e.g. port1.0.6) a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of ports and port ranges, e.g. port1.0.1, port1.0.4-1.0.6. Do not mix switch ports, static channel groups, and dynamic (LACP) channel groups in the same list</li></ul> |

**Mode** User Exec and Privileged Exec

**Usage** Note that any list of interfaces specified must not span any interfaces that are not installed.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the **show spanning-tree** command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

**Example** To display spanning tree information about port1.0.3, use the command:

```
awplus# show spanning-tree interface port1.0.3
```



**Output** Figure 12-2: Example output from the **show spanning-tree** command

```
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000000cd20f093
% 1: Bridge Id 80000000cd20f093
% 1: last topology change Sun Nov 20 12:24:24 1977
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% port1.0.3: Port 5023 - Id 839f - Role Designated - State Forwarding
% port1.0.3: Designated Path Cost 0
% port1.0.3: Configured Path Cost 200000 - Add type Explicit ref count 1
% port1.0.3: Designated Port Id 839f - Priority 128 -
% port1.0.3: Root 80000000cd20f093
% port1.0.3: Designated Bridge 80000000cd20f093
% port1.0.3: Message Age 0 - Max Age 20
% port1.0.3: Hello Time 2 - Forward Delay 15
% port1.0.3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
% port1.0.3: forward-transitions 32
% port1.0.3: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
% port1.0.3: No portfast configured - Current portfast off
% port1.0.3: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.3: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.3: no root guard configured - Current root guard off
% port1.0.3: Configured Link Type point-to-point - Current point-to-point
...
```

Figure 12-3: Example output from the **show spanning-tree** command in RSTP mode

```
awplus#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 - Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000000cd24ff2d
% 1: Bridge Id 80000000cd24ff2d
% 1: last topology change Thu Jul 26 02:06:26 2007
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% port1.0.1: Port 5001 - Id 8389 - Role Disabled - State Discarding
% port1.0.1: Designated Path Cost 0
% port1.0.1: Configured Path Cost 20000000 - Add type Explicit ref count 1
% port1.0.1: Designated Port Id 8389 - Priority 128 -
% port1.0.1: Root 80000000cd24ff2d
% port1.0.1: Designated Bridge 80000000cd24ff2d
% port1.0.1: Message Age 0 - Max Age 20
% port1.0.1: Hello Time 2 - Forward Delay 15
% port1.0.1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
% port1.0.1: forward-transitions 0
% port1.0.1: Version Rapid Spanning Tree Protocol - Received None - Send STP
% port1.0.1: No portfast configured - Current portfast off
% port1.0.1: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.1: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.1: no root guard configured - Current root guard off
% port1.0.1: Configured Link Type point-to-point - Current shared
%
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated Path Cost 0
% port1.0.2: Configured Path Cost 20000000 - Add type Explicit ref count 1
% port1.0.2: Designated Port Id 838a - Priority 128 -
% port1.0.2: Root 80000000cd24ff2d
% port1.0.2: Designated Bridge 80000000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 20
% port1.0.2: Hello Time 2 - Forward Delay 15
% port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
% port1.0.2: forward-transitions 0
% port1.0.2: Version Rapid Spanning Tree Protocol - Received None - Send STP
% port1.0.2: No portfast configured - Current portfast off
% port1.0.2: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.2: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.2: no root guard configured - Current root guard off
% port1.0.2: Configured Link Type point-to-point - Current shared
```

# show spanning-tree brief

**Overview** Use this command to display a summary of spanning tree status information on all ports. Use this command for RSTP, MSTP or STP.

**Syntax** show spanning-tree brief

| Parameter | Description                                   |
|-----------|-----------------------------------------------|
| brief     | A brief summary of spanning tree information. |

**Mode** User Exec and Privileged Exec

**Usage** Note that any list of interfaces specified must not span any interfaces that are not installed.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the **show spanning-tree** command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

**Example** To display a summary of spanning tree status information, use the command:

```
awplus# show spanning-tree brief
```

**Output** Figure 12-4: Example output from the **show spanning-tree brief** command

```
Default: Bridge up - Spanning Tree Enabled
Default: Root Path Cost 40000 - Root Port 4501 - Bridge Priority 32768
Default: Root Id 8000:0000cd250001
Default: Bridge Id 8000:0000cd296eb1
```

| Port      | Designated Bridge | Port Id | Role       | State      |
|-----------|-------------------|---------|------------|------------|
| sa1       | 8000:001577c9744b | 8195    | Rootport   | Forwarding |
| po1       | 8000:0000cd296eb1 | 81f9    | Designated | Forwarding |
| port1.0.1 | 8000:0000cd296eb1 | 8389    | Disabled   | Discarding |
| port1.0.2 | 8000:0000cd296eb1 | 838a    | Disabled   | Discarding |
| port1.0.3 | 8000:0000cd296eb1 | 838b    | Disabled   | Discarding |
| port1.0.4 | 8000:0000cd296eb1 | 838c    | Disabled   | Discarding |
| port1.0.5 | 8000:0000cd296eb1 | 838d    | Disabled   | Discarding |
| port1.0.6 | 8000:0000cd296eb1 | 838e    | Disabled   | Discarding |

**Related Commands** [show spanning-tree](#)

# show spanning-tree mst

**Overview** This command displays bridge-level information about the CIST and VLAN to MSTI mappings.

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 spanning-tree mst

**Mode** User Exec, Privileged Exec and Interface Configuration

**Example** To display bridge-level information about the CIST and VLAN to MSTI mappings, enter the command:

```
awplus# show spanning-tree mst
```

**Output** Figure 12-5: Example output from the **show spanning-tree mst** command

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000000475e93ffe
% 1: CIST Reg Root Id 8000000475e93ffe
% 1: CST Bridge Id 8000000475e93ffe
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%
% Instance VLAN
% 0: 1
% 2: 4
```

**Related Commands** [show spanning-tree mst interface](#)

# show spanning-tree mst config

**Overview** Use this command to display MSTP configuration identifier for the device.

**Syntax** show spanning-tree mst config

**Mode** User Exec, Privileged Exec and Interface Configuration

**Usage** The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

**Example** To display MSTP configuration identifier information, enter the command:

```
awplus# show spanning-tree mst config
```

**Output** Figure 12-6: Example output from the **show spanning-tree mst config** command

```
awplus#show spanning-tree mst config
%
% MSTP Configuration Information:
%-----
% Format Id : 0
% Name : My Name
% Revision Level : 0
% Digest : 0x80DEE46DA92A98CF21C603291B22880A
%-----
```

**Related Commands**

- [instance vlan \(MSTP\)](#)
- [region \(MSTP\)](#)
- [revision \(MSTP\)](#)

# show spanning-tree mst detail

**Overview** This command displays detailed information about each instance, and all interfaces associated with that particular instance.

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 spanning-tree mst detail

**Mode** User Exec, Privileged Exec and Interface Configuration

**Example** To display detailed information about each instance, and all interfaces associated with them, enter the command:

```
awplus# show spanning-tree mst detail
```

**Output** Figure 12-7: Example output from the **show spanning-tree mst detail** command

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% port1.0.1: Port 5001 - Id 8389 - Role Disabled - State Discarding
% port1.0.1: Designated External Path Cost 0 -Internal Path Cost 0
% port1.0.1: Configured Path Cost 20000000 - Add type Explicit ref count 1
% port1.0.1: Designated Port Id 8389 - CIST Priority 128 -
% port1.0.1: CIST Root 80000000cd24ff2d
% port1.0.1: Regional Root 80000000cd24ff2d
% port1.0.1: Designated Bridge 80000000cd24ff2d
% port1.0.1: Message Age 0 - Max Age 20
% port1.0.1: CIST Hello Time 2 - Forward Delay 15
% port1.0.1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
.
.
% port1.0.2: forward-transitions 0
% port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
% port1.0.2: No portfast configured - Current portfast off
% port1.0.2: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.2: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.2: no root guard configured - Current root guard off
% port1.0.2: Configured Link Type point-to-point - Current shared
%
% port1.0.3: Port 5003 - Id 838b - Role Disabled - State Discarding
% port1.0.3: Designated External Path Cost 0 -Internal Path Cost 0
% port1.0.3: Configured Path Cost 20000000 - Add type Explicit ref count 1
% port1.0.3: Designated Port Id 838b - CIST Priority 128 -
% port1.0.3: CIST Root 80000000cd24ff2d
% port1.0.3: Regional Root 80000000cd24ff2d
% port1.0.3: Designated Bridge 80000000cd24ff2d
% port1.0.3: Message Age 0 - Max Age 20
% port1.0.3: CIST Hello Time 2 - Forward Delay 15
% port1.0.3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
% port1.0.3: forward-transitions 0
% port1.0.3: Version Multiple Spanning Tree Protocol - Received None - Send STP
% port1.0.3: No portfast configured - Current portfast off
% port1.0.3: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.3: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.3: no root guard configured - Current root guard off
% port1.0.3: Configured Link Type point-to-point - Current shared
```

# show spanning-tree mst detail interface

**Overview** This command displays detailed information about the specified switch port, and the MST instances associated with it.

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 spanning-tree mst detail interface *<port>*

| Parameter           | Description                                                                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;port&gt;</i> | The port to display information about. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |

**Mode** User Exec, Privileged Exec and Interface Configuration

**Example** To display detailed information about port1.0.3 and the instances associated with it, enter the command:

```
awplus# show spanning-tree mst detail interface port1.0.3
```

**Output** Figure 12-8: Example output from the **show spanning-tree mst detail interface** command



```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated External Path Cost 0 - Internal Path Cost 0
% port1.0.2: Configured Path Cost 20000000 - Add type Explicit ref count 2
% port1.0.2: Designated Port Id 838a - CIST Priority 128 -
% port1.0.2: CIST Root 80000000cd24ff2d
% port1.0.2: Regional Root 80000000cd24ff2d
% port1.0.2: Designated Bridge 80000000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 20
% port1.0.2: CIST Hello Time 2 - Forward Delay 15
% port1.0.2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
% port1.0.2: forward-transitions 0
% port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
% port1.0.2: No portfast configured - Current portfast off
% port1.0.2: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.2: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.2: no root guard configured - Current root guard off
% port1.0.2: Configured Link Type point-to-point - Current shared
%
% Instance 2: Vlans: 2
% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated Internal Path Cost 0 - Designated Port Id 838a
% port1.0.2: Configured Internal Path Cost 20000000
% port1.0.2: Configured CST External Path cost 20000000
% port1.0.2: CST Priority 128 - MSTI Priority 128
% port1.0.2: Designated Root 80020000cd24ff2d
% port1.0.2: Designated Bridge 80020000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 0
% port1.0.2: Hello Time 2 - Forward Delay 15
% port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

# show spanning-tree mst instance

**Overview** This command displays detailed information for the specified instance, and all switch ports associated with that instance.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the [show spanning-tree](#) command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

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 spanning-tree mst instance *<instance>*

| Parameter               | Description                                   |
|-------------------------|-----------------------------------------------|
| <i>&lt;instance&gt;</i> | Specify an MSTP instance in the range <1-15>. |

**Mode** User Exec, Privileged Exec, and Interface Configuration

**Usage** To display detailed information for **instance 2**, and all switch ports associated with that instance, use the command:

```
awplus# show spanning-tree mst instance 2
```

**Output** Figure 12-9: Example output from the **show spanning-tree mst instance** command

```
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated Internal Path Cost 0 - Designated Port Id 838a
% port1.0.2: Configured Internal Path Cost 20000000
% port1.0.2: Configured CST External Path cost 20000000
% port1.0.2: CST Priority 128 - MSTI Priority 128
% port1.0.2: Designated Root 80020000cd24ff2d
% port1.0.2: Designated Bridge 80020000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 0
% port1.0.2: Hello Time 2 - Forward Delay 15
% port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

# show spanning-tree mst instance interface

**Overview** This command displays detailed information for the specified MST (Multiple Spanning Tree) instance, and the specified switch port associated with that MST instance.

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 spanning-tree mst instance *<instance>* interface *<port>*

| Parameter               | Description                                                                                                                                                             |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;instance&gt;</i> | Specify an MSTP instance in the range <1-15>.                                                                                                                           |
| <i>&lt;port&gt;</i>     | The port to display information about. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |

**Mode** User Exec, Privileged Exec, and Interface Configuration

**Example** To display detailed information for instance 2, interface port1.0.2, use the command:

```
awplus# show spanning-tree mst instance 2 interface port1.0.2
```

**Output** Figure 12-10: Example output from the **show spanning-tree mst instance** command

```
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated Internal Path Cost 0 - Designated Port Id 838a
% port1.0.2: Configured Internal Path Cost 20000000
% port1.0.2: Configured CST External Path cost 20000000
% port1.0.2: CST Priority 128 - MSTI Priority 128
% port1.0.2: Designated Root 80020000cd24ff2d
% port1.0.2: Designated Bridge 80020000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 0
% port1.0.2: Hello Time 2 - Forward Delay 15
% port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

# show spanning-tree mst interface

**Overview** This command displays the number of instances created, and VLANs associated with it for the specified switch port.

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 spanning-tree mst interface <port>

| Parameter | Description                                                                                                                                                             |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <port>    | The port to display information about. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |

**Mode** User Exec, Privileged Exec, and Interface Configuration

**Example** To display detailed information about each instance, and all interfaces associated with them, for port1.0.4, use the command:

```
awplus# show spanning-tree mst interface port1.0.4
```

**Output** Figure 12-11: Example output from the **show spanning-tree mst interface** command

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000008c73a2b22
% 1: CIST Reg Root Id 80000008c73a2b22
% 1: CST Bridge Id 80000008c73a2b22
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%
% Instance VLAN
% 0: 1
% 1: 2-3
% 2: 4-5
```

# show spanning-tree mst detail interface

**Overview** This command displays detailed information about the specified switch port, and the MST instances associated with it.

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 spanning-tree mst detail interface *<port>*

| Parameter           | Description                                                                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;port&gt;</i> | The port to display information about. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |

**Mode** User Exec, Privileged Exec and Interface Configuration

**Example** To display detailed information about port1.0.3 and the instances associated with it, enter the command:

```
awplus# show spanning-tree mst detail interface port1.0.3
```

**Output** Figure 12-12: Example output from the **show spanning-tree mst detail interface** command

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated External Path Cost 0 - Internal Path Cost 0
% port1.0.2: Configured Path Cost 20000000 - Add type Explicit ref count 2
% port1.0.2: Designated Port Id 838a - CIST Priority 128 -
% port1.0.2: CIST Root 80000000cd24ff2d
% port1.0.2: Regional Root 80000000cd24ff2d
% port1.0.2: Designated Bridge 80000000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 20
% port1.0.2: CIST Hello Time 2 - Forward Delay 15
% port1.0.2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
% port1.0.2: forward-transitions 0
% port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
% port1.0.2: No portfast configured - Current portfast off
% port1.0.2: portfast bpdu-guard default - Current portfast bpdu-guard off
% port1.0.2: portfast bpdu-filter default - Current portfast bpdu-filter off
% port1.0.2: no root guard configured - Current root guard off
% port1.0.2: Configured Link Type point-to-point - Current shared
%
% Instance 2: Vlans: 2
% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
% port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
% port1.0.2: Designated Internal Path Cost 0 - Designated Port Id 838a
% port1.0.2: Configured Internal Path Cost 20000000
% port1.0.2: Configured CST External Path cost 20000000
% port1.0.2: CST Priority 128 - MSTI Priority 128
% port1.0.2: Designated Root 80020000cd24ff2d
% port1.0.2: Designated Bridge 80020000cd24ff2d
% port1.0.2: Message Age 0 - Max Age 0
% port1.0.2: Hello Time 2 - Forward Delay 15
% port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

# show spanning-tree statistics

**Overview** This command displays BPDU (Bridge Protocol Data Unit) statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances.

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 spanning-tree statistics

**Mode** Privileged Exec

**Usage** To display BPDU statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances, use the command:

```
awplus# show spanning-tree statistics
```

**Output** Figure 12-13: Example output from the **show spanning-tree statistics** command

```

Port
number = 915 Interface = port1.0.6
=====
% BPDU Related Parameters
% -----
% Port Spanning Tree : Disable
% Spanning Tree Type : Rapid Spanning Tree Protocol
% Current Port State : Discarding
% Port ID : 8393
% Port Number : 393
% Path Cost : 20000000
% Message Age : 0
% Designated Root : ec:cd:6d:20:c0:ed
% Designated Cost : 0
% Designated Bridge : ec:cd:6d:20:c0:ed
% Designated Port Id : 8393
% Top Change Ack : FALSE
% Config Pending : FALSE
% PORT Based Information & Statistics
% -----
% Config Bpdu's xmitted : 0
% Config Bpdu's received : 0
% TCN Bpdu's xmitted : 0
% TCN Bpdu's received : 0
% Forward Trans Count : 0
% STATUS of Port Timers
% -----
% Hello Time Configured : 2
% Hello timer : INACTIVE
% Hello Time Value : 0
% Forward Delay Timer : INACTIVE
% Forward Delay Timer Value : 0
% Message Age Timer : INACTIVE
% Message Age Timer Value : 0
% Topology Change Timer : INACTIVE
% Topology Change Timer Value : 0
% Hold Timer : INACTIVE
% Hold Timer Value : 0
% Other Port-Specific Info
% -----
% Max Age Transitions : 1
% Msg Age Expiry : 0
% Similar BPDUS Rcvd : 0
% Src Mac Count : 0
% Total Src Mac Rcvd : 0
% Next State : Learning
% Topology Change Time : 0

```



# show spanning-tree statistics instance

**Overview** This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance, and all switch ports associated with that MST instance.

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 spanning-tree statistics instance *<instance>*

| Parameter               | Description                                   |
|-------------------------|-----------------------------------------------|
| <i>&lt;instance&gt;</i> | Specify an MSTP instance in the range <1-15>. |

**Mode** Privileged Exec

**Usage** To display BPDU statistics information for MST instance 2, and all switch ports associated with that MST instance, use the command:

```
awplus# show spanning-tree statistics instance 2
```

**Output** Figure 12-14: Example output from the **show spanning-tree statistics instance** command:

```
% % INST_PORT port1.0.3 Information & Statistics
% -----
% Config Bpdu's xmitted (port/inst) : (0/0)
% Config Bpdu's received (port/inst) : (0/0)
% TCN Bpdu's xmitted (port/inst) : (0/0)
% TCN Bpdu's received (port/inst) : (0/0)
% Message Age(port/Inst) : (0/0)
% port1.0.3: Forward Transitions : 0
% Next State : Learning
% Topology Change Time : 0
% INST_PORT port1.0.4 Information & Statistics
% -----
% Config Bpdu's xmitted (port/inst) : (0/0)
% Config Bpdu's received (port/inst) : (0/0)
% TCN Bpdu's xmitted (port/inst) : (0/0)
% TCN Bpdu's received (port/inst) : (0/0)
% Message Age(port/Inst) : (0/0)
% port1.0.4: Forward Transitions : 0
% Next State : Learning
% Topology Change Time : 0
% INST_PORT port1.0.5 Information & Statistics
% -----
% Config Bpdu's xmitted (port/inst) : (0/0)
% Config Bpdu's received (port/inst) : (0/0)
% TCN Bpdu's xmitted (port/inst) : (0/0)
% TCN Bpdu's received (port/inst) : (0/0)
% Message Age(port/Inst) : (0/0)
% port1.0.5: Forward Transitions : 0
% Next State : Learning
% Topology Change Time : 0%
```

**Related Commands** [show spanning-tree statistics](#)

# show spanning-tree statistics instance interface

**Overview** This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance and the specified switch port associated with that MST instance.

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 spanning-tree statistics instance *<instance>* interface *<port>*

| Parameter               | Description                                                                                                                                                             |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;instance&gt;</i> | Specify an MSTP instance in the range <1-15>.                                                                                                                           |
| <i>&lt;port&gt;</i>     | The port to display information about. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |

**Mode** Privileged Exec

**Example** To display BPDU statistics for MST instance 2, interface port1.0.2, use the command:

```
awplus# show spanning-tree statistics instance 2 interface port1.0.2
```

**Output** Figure 12-15: Example output from the **show spanning-tree statistics instance interface** command

```
awplus#sh spanning-tree statistics interface port1.0.2 instance 1
Spanning Tree Enabled for Instance : 1
=====
% INST_PORT port1.0.2 Information & Statistics
% -----
% Config Bpdu's xmitted (port/inst) : (0/0)
% Config Bpdu's received (port/inst) : (0/0)
% TCN Bpdu's xmitted (port/inst) : (0/0)
% TCN Bpdu's received (port/inst) : (0/0)
% Message Age(port/Inst) : (0/0)
% port1.0.2: Forward Transitions : 0
% Next State : Learning
% Topology Change Time : 0

% Other Inst/Vlan Information & Statistics
% -----
% Bridge Priority : 0
% Bridge Mac Address : ec:cd:6d:20:c0:ed
% Topology Change Initiator : 5023
% Last Topology Change Occured : Mon Aug 22 05:42:06 2011
% Topology Change : FALSE
% Topology Change Detected : FALSE
% Topology Change Count : 1
% Topology Change Last Recvd from : 00:00:00:00:00:00
```

**Related Commands** [show spanning-tree statistics](#)

# show spanning-tree statistics interface

**Overview** This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified switch port, and all MST instances associated with that switch port.

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 spanning-tree statistics interface *<port>*

| Parameter           | Description                                                                                                                                                             |
|---------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;port&gt;</i> | The port to display information about. The port may be a switch port (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2). |

**Mode** Privileged Exec

**Example** To display BPDU statistics about each MST instance for port1.0.4, use the command:

```
awplus# show spanning-tree statistics interface port1.0.4
```

**Output** Figure 12-16: Example output from the **show spanning-tree statistics interface** command

```
awplus#show
spanning-tree statistics interface port1.0.2

 Port number = 906 Interface = port1.0.2

 =====
% BPDU Related Parameters
% -----
% Port Spanning Tree : Disable
% Spanning Tree Type : Multiple Spanning Tree Protocol
% Current Port State : Discarding
% Port ID : 838a
% Port Number : 38a
% Path Cost : 200000000
% Message Age : 0
% Designated Root : ec:cd:6d:20:c0:ed
% Designated Cost : 0
% Designated Bridge : ec:cd:6d:20:c0:ed
% Designated Port Id : 838a
% Top Change Ack : FALSE
% Config Pending : FALSE

% PORT Based Information& Statistics
% -----
% Config Bpdu's xmitted : 0
% Config Bpdu's received : 0
% TCN Bpdu's xmitted : 0
% TCN Bpdu's received : 0
% Forward Trans Count : 0

% STATUS of Port Timers
% -----
% Hello Time Configured : 2
% Hello timer : INACTIVE
% Hello Time Value : 0
% Forward Delay Timer : INACTIVE
% Forward Delay Timer Value : 0
% Message Age Timer : INACTIVE
% Message Age Timer Value : 0
% Topology Change Timer : INACTIVE
% Topology Change Timer Value : 0
% Hold Timer : INACTIVE
% Hold Timer Value : 0

% Other Port-Specific Info
% -----
% Max Age Transitions : 1
% Msg Age Expiry : 0
% Similar BPDUS Rcvd : 0
% Src Mac Count : 0
% Total Src Mac Rcvd : 0
% Next State : Learning
% Topology Change Time : 0
```

```
% Other Bridge information & Statistics

% STP Multicast Address : 01:80:c2:00:00:00
% Bridge Priority : 32768
% Bridge Mac Address : ec:cd:6d:20:c0:ed
% Bridge Hello Time : 2
% Bridge Forward Delay : 15
% Topology Change Initiator : 5023
% Last Topology Change Occured : Mon Aug 22 05:41:20 2011
% Topology Change : FALSE
% Topology Change Detected : TRUE
% Topology Change Count : 1
% Topology Change Last Recvd from : 00:00:00:00:00:00
```

**Related** [show spanning-tree statistics](#)  
**Commands**

# show spanning-tree vlan range-index

**Overview** Use this command to display information about MST (Multiple Spanning Tree) instances and the VLANs associated with them including the VLAN range-index value for the device.

**Syntax** show spanning-tree vlan range-index

**Mode** Privileged Exec

**Example** To display information about MST instances and the VLANs associated with them for the device, including the VLAN range-index value, use the following command:

```
awplus# show spanning-tree vlan range-index
```

**Output** Figure 12-17: Example output from the **show spanning-tree vlan range-index** command

```
awplus#show spanning-tree vlan range-index
% MST Instance VLAN RangeIdx
% 1 1 1
%
```

**Related Commands** [show spanning-tree statistics](#)



# spanning-tree autoedge (RSTP and MSTP)

**Overview** Use this command to enable the autoedge feature on the port.

The autoedge feature allows the port to automatically detect that it is an edge port. If it does not receive any BPDUs in the first three seconds after linkup, enabling, or entering RSTP or MSTP mode, it sets itself to be an edgeport and enters the forwarding state.

Use this command for RSTP or MSTP.

Use the **no** variant of this command to disable this feature.

**Syntax** spanning-tree autoedge  
no spanning-tree autoedge

**Default** Disabled

**Mode** Interface Configuration

**Example** awplus# configure terminal  
awplus(config)# interface port1.0.3  
awplus(config-if)# spanning-tree autoedge

**Related Commands** [spanning-tree edgeport \(RSTP and MSTP\)](#)

## spanning-tree bpdudata-bbox="164 158 883 205" data-label="Text"> **Overview** Use this command in Global Configuration mode to configure BPDU (Bridge Protocol Data Unit) discarding or forwarding, with STP (Spanning Tree Protocol) disabled on the switch.

See the Usage note about disabling Spanning Tree before using this command, and using this command to forward unsupported BPDUs unchanged for unsupported STP Protocols.

There is not a **no** variant for this command. Instead, apply the **discard** parameter to reset it back to the default then re-enable STP with **spanning-tree enable** command.

**Syntax** spanning-tree bpdudata-bbox="262 378 891 621" data-label="Table">

| Parameter                                                                                                                                                                                                                                           | Description                                                                                                    |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| bpdudata-bbox="404 406 873 450" data-label="Text"> <p>A port that has BPDU filtering enabled will not transmit any BPDUs and will ignore any BPDUs received. This port type has one of the following parameters (in Global Configuration mode):</p> |                                                                                                                |
| discard                                                                                                                                                                                                                                             | Discards all ingress STP BPDU frames.                                                                          |
| forward                                                                                                                                                                                                                                             | Forwards any ingress STP BPDU packets to all ports, regardless of any VLAN membership.                         |
| forward -<br>untagged -<br>vlan                                                                                                                                                                                                                     | Forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port's native VLAN. |
| forward -<br>vlan                                                                                                                                                                                                                                   | Forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port's native VLAN.   |

| bpdudata-bbox="404 406 873 450" data-label="Text"> A port that has BPDU filtering enabled will not transmit any BPDUs and will ignore any BPDUs received. This port type has one of the following parameters (in Global Configuration mode): |
| discard | Discards all ingress STP BPDU frames. |
| forward | Forwards any ingress STP BPDU packets to all ports, regardless of any VLAN membership. |
| forward - untagged - vlan | Forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port's native VLAN. |
| forward - vlan | Forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port's native VLAN. |

**Default** The discard parameter is enabled by default.

**Mode** Global Configuration

**Usage** You must first disable Spanning Tree with the **spanning-tree enable** command before you can use this command to then configure BPDU discarding or forwarding.

This command enables the switch to forward unsupported BPDUs with an unsupported Spanning Tree Protocol, such as proprietary STP protocols with unsupported BPDUs, by forwarding BPDU (Bridge Protocol Data Unit) frames unchanged through the switch.

When you want to revert to default behavior on the switch, issue a **spanning-tree bdpudiscard** command and re-enable Spanning Tree with a **s panning-tree enable** command.

**Examples** To enable STP BPDU discard in Global Configuration mode with STP disabled, which discards all ingress STP BPDU frames, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu discard
```

To enable STP BPDU forward in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports regardless of any VLAN membership, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward
```

To enable STP BPDU forwarding for untagged frames in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port's native VLAN, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward-untagged-vlan
```

To enable STP BPDU forwarding for tagged frames in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port's native VLAN, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward-vlan
```

To reset STP BPDU back to the default discard parameter and re-enable STP on the switch, enter the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree bpdu discard
awplus(config)# spanning-tree stp enable
```

**Related  
Commands** [show spanning-tree](#)  
[spanning-tree enable](#)

# spanning-tree cisco-interoperability (MSTP)

**Overview** Use this command to enable/disable Cisco-interoperability for MSTP.  
Use this command for MSTP only.

**Syntax** spanning-tree cisco-interoperability {enable|disable}

| Parameter | Description                              |
|-----------|------------------------------------------|
| enable    | Enable Cisco interoperability for MSTP.  |
| disable   | Disable Cisco interoperability for MSTP. |

**Default** If this command is not used, Cisco interoperability is disabled.

**Mode** Global Configuration

**Usage** For compatibility with certain Cisco devices, all devices in the switched LAN running the AlliedWare Plus™ Operating System must have Cisco-interoperability enabled. When the AlliedWare Plus Operating System is interoperating with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN to instance mapping is not used to classify regions when interoperating with Cisco.

**Examples** To enable Cisco interoperability on a Layer 2 device:

```
awplus# configure terminal
awplus(config)# spanning-tree cisco-interoperability enable
```

To disable Cisco interoperability on a Layer 2 device:

```
awplus# configure terminal
awplus(config)# spanning-tree cisco-interoperability disable
```

# spanning-tree edgeport (RSTP and MSTP)

**Overview** Use this command to set a port as an edge-port.

Use this command for RSTP or MSTP.

This command has the same effect as the [spanning-tree portfast \(STP\)](#) command, but the configuration displays differently in the output of some show commands.

Use the **no** variant of this command to set a port to its default state (not an edge-port).

**Syntax** spanning-tree edgeport  
no spanning-tree edgeport

**Default** Not an edge port.

**Mode** Interface Configuration

**Usage** Use this command on a switch port connected to a LAN that has no other bridges attached. If a BPDU is received on the port that indicates that another bridge is connected to the LAN, then the port is no longer treated as an edge port.

**Example** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# spanning-tree edgeport

**Related Commands** [spanning-tree autoedge \(RSTP and MSTP\)](#)

# spanning-tree enable

**Overview** Use this command in Global Configuration mode to enable the specified spanning tree protocol for all switch ports. Note that this must be the spanning tree protocol that is configured on the device by the [spanning-tree mode](#) command.

Use the **no** variant of this command to disable the configured spanning tree protocol. This places all switch ports in the forwarding state.

**Syntax** `spanning-tree {mstp|rstp|stp} enable`  
`no spanning-tree {mstp|rstp|stp} enable`

| Parameter | Description                                                 |
|-----------|-------------------------------------------------------------|
| mstp      | Enables or disables MSTP (Multiple Spanning Tree Protocol). |
| rstp      | Enables or disables RSTP (Rapid Spanning Tree Protocol).    |
| stp       | Enables or disables STP (Spanning Tree Protocol).           |

**Default** RSTP is enabled by default for all switch ports.

**Mode** Global Configuration

**Usage** With no configuration, spanning tree is enabled, and the spanning tree mode is set to RSTP. To change the mode, see [spanning-tree mode](#) command.

**Examples** To enable STP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree stp enable
```

To disable STP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
```

To enable MSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mstp enable
```

To disable MSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree mstp enable
```

To enable RSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree rstp enable
```

To disable RSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
```

```
awplus(config)# no spanning-tree rstp enable
```

**Related  
Commands**

[spanning-tree bpdu](#)

[spanning-tree mode](#)

# spanning-tree errdisable-timeout enable

**Overview** Use this command to enable the errdisable-timeout facility, which sets a timeout for ports that are disabled due to the BPDU guard feature.

Use this command for RSTP or MSTP.

Use the **no** variant of this command to disable the errdisable-timeout facility.

**Syntax** spanning-tree errdisable-timeout enable  
no spanning-tree errdisable-timeout enable

**Default** By default, the errdisable-timeout is disabled.

**Mode** Global Configuration

**Usage** The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port. This command associates a timer with the feature such that the port is re-enabled without manual intervention after a set interval. This interval can be configured by the user using the [spanning-tree errdisable-timeout interval](#) command.

**Example** awplus# configure terminal  
awplus(config)# spanning-tree errdisable-timeout enable

**Related Commands** [show spanning-tree](#)  
[spanning-tree errdisable-timeout interval](#)  
[spanning-tree portfast bpdu-guard](#)



# spanning-tree errdisable-timeout interval

**Overview** Use this command to specify the time interval after which a port is brought back up when it has been disabled by the BPDU guard feature.

Use this command for RSTP or MSTP.

**Syntax** spanning-tree errdisable-timeout interval *<10-1000000>*  
no spanning-tree errdisable-timeout interval

| Parameter                 | Description                                         |
|---------------------------|-----------------------------------------------------|
| <i>&lt;10-1000000&gt;</i> | Specify the errdisable-timeout interval in seconds. |

**Default** By default, the port is re-enabled after 300 seconds.

**Mode** Global Configuration

**Example** awplus# configure terminal  
awplus(config)# spanning-tree errdisable-timeout interval 34

**Related Commands** [show spanning-tree](#)  
[spanning-tree errdisable-timeout enable](#)  
[spanning-tree portfast bpdu-guard](#)

# spanning-tree force-version

**Overview** Use this command in Interface Configuration mode for a switch port interface only to force the protocol version for the switch port. Use this command for RSTP or MSTP only.

**Syntax** spanning-tree force-version *<version>*  
no spanning-tree force-version

| Parameter              | Description                                                                                                                                                                            |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;version&gt;</i> | <i>&lt;0 - 3&gt;</i> Version identifier.                                                                                                                                               |
| 0                      | Forces the port to operate in STP mode.                                                                                                                                                |
| 1                      | Not supported.                                                                                                                                                                         |
| 2                      | Forces the port to operate in RSTP mode. If it receives STP BPDUs, it can automatically revert to STP mode.                                                                            |
| 3                      | Forces the port to operate in MSTP mode (this option is only available if MSTP mode is configured). If it receives RSTP or STP BPDUs, it can automatically revert to RSTP or STP mode. |

**Default** By default, no version is forced for the port. The port is in the spanning tree mode configured for the device, or a lower version if it automatically detects one.

**Mode** Interface Configuration mode for a switch port interface only.

**Examples** Set the value to enforce the spanning tree protocol (STP):

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree force-version 0
```

Set the default protocol version:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree force-version
```

**Related Commands** [show spanning-tree](#)

# spanning-tree forward-time

**Overview** Use this command to set the forward delay value. Use the **no** variant of this command to reset the forward delay value to the default setting of 15 seconds.

The **forward delay** sets the time (in seconds) to control how fast a port changes its spanning tree state when moving towards the forwarding state. If the mode is set to STP, the value determines how long the port stays in each of the listening and learning states which precede the forwarding state. If the mode is set to RSTP or MSTP, this value determines the maximum time taken to transition from discarding to learning and from learning to forwarding.

This value is used only when the device is acting as the root bridge. Devices not acting as the Root Bridge use a dynamic value for the **forward delay** set by the root bridge. The **forward delay**, **max-age**, and **hello time** parameters are interrelated.

**Syntax** spanning-tree forward-time <forward-delay>  
no spanning-tree forward-time

| Parameter       | Description                                  |
|-----------------|----------------------------------------------|
| <forward-delay> | <4-30> The forwarding time delay in seconds. |

**Default** The default is 15 seconds.

**Mode** Global Configuration

**Usage** The allowable range for forward-time is 4-30 seconds.

The **forward delay**, **max-age**, and **hello time** parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

$2 \times (\text{forward delay} - 1.0 \text{ seconds}) \geq \text{max-age}$

$\text{max-age} \geq 2 \times (\text{hello time} + 1.0 \text{ seconds})$

**Example** awplus# configure terminal  
awplus(config)# spanning-tree forward-time 6

**Related Commands** show spanning-tree  
spanning-tree forward-time  
spanning-tree hello-time  
spanning-tree mode

# spanning-tree guard root

**Overview** Use this command in Interface Configuration mode for a switch port only to enable the Root Guard feature for the switch port. The root guard feature disables reception of superior BPDUs. You can use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to disable the root guard feature for the port.

**Syntax** spanning-tree guard root  
no spanning-tree guard root

**Mode** Interface Configuration mode for a switch port interface only.

**Usage** The Root Guard feature makes sure that the port on which it is enabled is a designated port. If the Root Guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

**Example** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# spanning-tree guard root

# spanning-tree hello-time

**Overview** Use this command to set the hello-time. This sets the time in seconds between the transmission of device spanning tree configuration information when the device is the Root Bridge of the spanning tree or is trying to become the Root Bridge.

Use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to restore the default of the hello time.

**Syntax** spanning-tree hello-time *<hello-time>*  
no spanning-tree hello-time

| Parameter                 | Description                                |
|---------------------------|--------------------------------------------|
| <i>&lt;hello-time&gt;</i> | <1-10> The hello BPDU interval in seconds. |

**Default** Default is 2 seconds.

**Mode** Global Configuration and Interface Configuration for switch ports.

**Usage** The allowable range of values is 1-10 seconds.  
The forward delay, max-age, and hello time parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

$2 \times (\text{forward delay} - 1.0 \text{ seconds}) \geq \text{max-age}$

$\text{max-age} \geq 2 \times (\text{hello time} + 1.0 \text{ seconds})$

**Example** awplus# configure terminal  
awplus(config)# spanning-tree hello-time 3

**Related Commands** spanning-tree forward-time  
spanning-tree max-age  
show spanning-tree

## spanning-tree link-type

**Overview** Use this command in Interface Configuration mode for a switch port interface only to enable or disable point-to-point or shared link types on the switch port.

Use this command for RSTP or MSTP only.

Use the **no** variant of this command to return the port to the default link type.

**Syntax** spanning-tree link-type {point-to-point|shared}  
no spanning-tree link-type

| Parameter      | Description               |
|----------------|---------------------------|
| shared         | Disable rapid transition. |
| point-to-point | Enable rapid transition.  |

**Default** The default link type is point-to-point.

**Mode** Interface Configuration mode for a switch port interface only.

**Usage** You may want to set link type to shared if the port is connected to a hub with multiple devices connected to it.

**Examples** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# spanning-tree link-type point-to-point

# spanning-tree max-age

**Overview** Use this command to set the max-age. This sets the maximum age, in seconds, that dynamic spanning tree configuration information is stored in the device before it is discarded.

Use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to restore the default of max-age.

**Syntax** spanning-tree max-age <max-age>  
no spanning-tree max-age

| Parameter | Description                          |
|-----------|--------------------------------------|
| <max-age> | <6-40> The maximum time, in seconds. |

**Default** The default of spanning-tree max-age is 20 seconds.

**Mode** Global Configuration

**Usage** Max-age is the maximum time in seconds for which a message is considered valid. Configure this value sufficiently high, so that a frame generated by the root bridge can be propagated to the leaf nodes without exceeding the max-age.

The **forward delay**, **max-age**, and **hello time** parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

$2 \times (\text{forward delay} - 1.0 \text{ seconds}) \geq \text{max-age}$

$\text{max-age} \geq 2 \times (\text{hello time} + 1.0 \text{ seconds})$

**Example** awplus# configure terminal  
awplus(config)# spanning-tree max-age 12

**Related Commands** [show spanning-tree](#)  
[spanning-tree forward-time](#)  
[spanning-tree hello-time](#)

## spanning-tree max-hops (MSTP)

**Overview** Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST region.

Use the **no** variant of this command to restore the default.

Use this command for MSTP only.

**Syntax** spanning-tree max-hops *<hop-count>*  
no spanning-tree max-hops *<hop-count>*

| Parameter                | Description                                                              |
|--------------------------|--------------------------------------------------------------------------|
| <i>&lt;hop-count&gt;</i> | Specify the maximum hops the BPDU will be valid for in the range <1-40>. |

**Default** The default max-hops in a MST region is 20.

**Mode** Global Configuration

**Usage** Specifying the max hops for a BPDU prevents the messages from looping indefinitely in the network. The hop count is decremented by each receiving port. When a device receives an MST BPDU that has a hop count of zero, it discards the BPDU.

**Examples** awplus# configure terminal  
awplus(config)# spanning-tree max-hops 25  
awplus# configure terminal  
awplus(config)# no spanning-tree max-hops



# spanning-tree mode

**Overview** Use this command to change the spanning tree protocol mode on the device. The spanning tree protocol mode on the device can be configured to either STP, RSTP or MSTP.

**Syntax** `spanning-tree mode {stp|rstp|mstp}`

**Default** The default spanning tree protocol mode on the device is RSTP.

**Mode** Global Configuration

**Usage** With no configuration, the device will have spanning tree enabled, and the spanning tree mode will be set to RSTP. Use this command to change the spanning tree protocol mode on the device. MSTP is VLAN aware, but RSTP and STP are not VLAN aware. To enable or disable spanning tree operation, see the [spanning-tree enable](#) command.

**Examples** To change the spanning tree mode from the default of RSTP to MSTP, use the following commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
```

**Related Commands** [spanning-tree enable](#)

# spanning-tree mst configuration

**Overview** Use this command to enter the MST Configuration mode to configure the Multiple Spanning-Tree Protocol.

**Syntax** spanning-tree mst configuration

**Mode** Global Configuration

**Examples** The following example uses this command to enter MST Configuration mode. Note the change in the command prompt.

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)#
```

# spanning-tree mst instance

**Overview** Use this command in Interface Configuration mode to assign a Multiple Spanning Tree instance (MSTI) to a switch port or channel group.

Note that ports are automatically configured to send and receive spanning-tree information for the associated MSTI when VLANs are assigned to MSTIs using the [instance vlan \(MSTP\)](#) command.

Use the **no** variant of this command in Interface Configuration mode to remove the MSTI from the specified switch port or channel group.

**Syntax** spanning-tree mst instance <instance-id>  
no spanning-tree mst instance <instance-id>

| Parameter     | Description                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <instance-id> | <1-15> Specify the MST instance ID. The MST instance must have already been created using the <a href="#">instance vlan (MSTP)</a> command. |

**Default** A port automatically becomes a member of an MSTI when it is assigned to a VLAN.

**Mode** Interface Configuration mode for a switch port or channel group.

**Usage** You can disable automatic configuration of member ports of a VLAN to an associated MSTI by using a **no spanning-tree mst instance** command to remove the member port from the MSTI. Use the **spanning-tree mst instance** command to add a VLAN member port back to the MSTI.

**Examples** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# spanning-tree mst instance 3  
awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# no spanning-tree mst instance 3

**Related Commands** [instance vlan \(MSTP\)](#)  
[spanning-tree mst instance path-cost](#)  
[spanning-tree mst instance priority](#)  
[spanning-tree mst instance restricted-role](#)  
[spanning-tree mst instance restricted-tcn](#)

# spanning-tree mst instance path-cost

**Overview** Use this command in Interface Configuration mode for a switch port interface only to set the cost of a path associated with a switch port, for the specified MSTI (Multiple Spanning Tree Instance) identifier.

This specifies the switch port's contribution to the cost of a path to the MSTI regional root via that port. This applies when the port is the root port for the MSTI.

Use the **no** variant of this command to restore the default cost value of the path.

**Syntax** spanning-tree mst instance *<instance-id>* path-cost *<path-cost>*  
no spanning-tree mst instance *<instance-id>* path-cost

| Parameter                  | Description                                                                                                                                                  |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;instance-id&gt;</i> | Specify the MSTI identifier in the range <1-15>.                                                                                                             |
| <i>&lt;path-cost&gt;</i>   | Specify the cost of path in the range of <1 - 2000000000>, where a lower path-cost indicates a greater likelihood of the specific interface becoming a root. |

**Default** The default path cost values and the range of recommended path cost values depend on the port speed, as shown in the following table from the IEEE 802.1q-2003 standard.

| Port speed         | Default path cost | Recommended path cost range |
|--------------------|-------------------|-----------------------------|
| Less than 100 Kb/s | 200,000,000       | 20,000,000-200,000,000      |
| 1Mbps              | 20,000,000        | 2,000,000-20,000,000        |
| 10Mbps             | 2,000,000         | 200,000-2,000,000           |
| 100 Mbps           | 200,000           | 20,000-200,000              |
| 1 Gbps             | 20,000            | 2,000-20,000                |
| 10 Gbps            | 2,000             | 200-2,000                   |
| 100 Gbps           | 200               | 20-200                      |
| 1Tbps              | 20                | 2-200                       |
| 10 Tbps            | 2                 | 2-20                        |

**Mode** Interface Configuration mode for a switch port interface only.

**Usage** Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the spanning-tree instance command.

**Examples**   awplus# configure terminal  
              awplus(config)# interface port1.0.2  
              awplus(config-if)# spanning-tree mst instance 3 path-cost 1000  
              awplus# configure terminal  
              awplus(config)# interface port1.0.2  
              awplus(config-if)# no spanning-tree mst instance 3 path-cost

**Related  
Commands**   instance vlan (MSTP)  
              spanning-tree mst instance  
              spanning-tree mst instance priority  
              spanning-tree mst instance restricted-role  
              spanning-tree mst instance restricted-tcn

# spanning-tree mst instance priority

**Overview** Use this command in Interface Configuration mode for a switch port interface only to set the port priority for an MST instance (MSTI).

Use the **no** variant of this command to restore the default priority value (128).

**Syntax** spanning-tree mst instance *<instance-id>* priority *<priority>*  
no spanning-tree mst instance *<instance-id>* [priority]

| Parameter                  | Description                                                                                                                                   |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;instance-id&gt;</i> | Specify the MSTI identifier in the range <1-15>.                                                                                              |
| <i>&lt;priority&gt;</i>    | This must be a multiple of 16 and within the range <0-240>. A lower priority indicates greater likelihood of the port becoming the root port. |

**Default** The default is 128.

**Mode** Interface Configuration mode for a switch port interface.

**Usage** This command sets the value of the priority field contained in the port identifier. The MST algorithm uses the port priority when determining the root port for the switch in the MSTI. The port with the lowest value is considered to have the highest priority and will be chosen as root port over a port - equivalent in all other aspects - but with a higher priority value.

**Examples** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# spanning-tree mst instance 3 priority 112  
awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# no spanning-tree mst instance 3 priority

**Related Commands** instance vlan (MSTP)  
spanning-tree priority (port priority)  
spanning-tree mst instance  
spanning-tree mst instance path-cost  
spanning-tree mst instance restricted-role  
spanning-tree mst instance restricted-tcn

# spanning-tree mst instance restricted-role

**Overview** Use this command in Interface Configuration mode for a switch port interface only to enable the restricted role for an MSTI (Multiple Spanning Tree Instance) on a switch port. Configuring the restricted role for an MSTI on a switch port prevents the switch port from becoming the root port in a spanning tree topology.

Use the **no** variant of this command to disable the restricted role for an MSTI on a switch port. Removing the restricted role for an MSTI on a switch port allows the switch port to become the root port in a spanning tree topology.

**Syntax** spanning-tree mst instance *<instance-id>* restricted-role  
no spanning-tree mst instance *<instance-id>* restricted-role

| Parameter                  | Description                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;instance-id&gt;</i> | <1-15> Specify the MST instance ID. The MST instance must have already been created using the <a href="#">instance vlan (MSTP)</a> command. |

**Default** The restricted role for an MSTI instance on a switch port is disabled by default.

**Mode** Interface Configuration mode for a switch port interface only.

**Usage** The root port is the port providing the best path from the bridge to the root bridge. Use this command to disable a port from becoming a root port. Use the **no** variant of this command to enable a port to become a root port. See the [STP Feature Overview and Configuration Guide](#) for root port information.

**Examples**

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 restricted-role
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
restricted-role
```

**Related Commands**

- [instance vlan \(MSTP\)](#)
- [spanning-tree priority \(port priority\)](#)
- [spanning-tree mst instance](#)
- [spanning-tree mst instance path-cost](#)
- [spanning-tree mst instance restricted-tcn](#)

# spanning-tree mst instance restricted-tcn

**Overview** Use this command in Interface Configuration mode for a switch port interface only to set the restricted TCN (Topology Change Notification) value to TRUE for the specified MSTI (Multiple Spanning Tree Instance).

Use the **no** variant of this command in Interface Configuration mode to reset the restricted TCN for the specified MSTI to the default value of FALSE.

**Syntax** spanning-tree mst instance *<instance-id>* restricted-tcn  
no spanning-tree mst instance *<instance-id>* restricted-tcn

| Parameter                  | Description                                                                                                                                 |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;instance-id&gt;</i> | <1-15> Specify the MST instance ID. The MST instance must have already been created using the <a href="#">instance vlan (MSTP)</a> command. |

**Default** The default value for restricted TCNs is FALSE, as reset with the **no** variant of this command.

**Mode** Interface Configuration mode for a switch port interface only.

**Usage** A Topology Change Notification (TCN) is a simple Bridge Protocol Data Unit (BPDU) that a bridge sends out to its root port to signal a topology change. You can configure restricted TCN between TRUE and FALSE values with this command and the **no** variant of this command.

If you configure restricted TCN to TRUE with this command then this stops the switch port from propagating received topology change notifications and topology changes to other switch ports.

If you configure restricted TCN to FALSE with the **no** variant of this command then this enables the switch port to propagate received topology change notifications and topology changes to other switch ports.

**Examples**

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 restricted-tcn
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
restricted-tcn
```



**Related  
Commands**

- instance vlan (MSTP)
- spanning-tree priority (port priority)
- spanning-tree mst instance
- spanning-tree mst instance path-cost
- spanning-tree mst instance restricted-role

# spanning-tree path-cost

**Overview** Use this command in Interface Configuration mode for a switch port interface only to set the cost of a path for the specified port. This value then combines with others along the path to the root bridge in order to determine the total cost path value from the particular port, to the root bridge. The lower the numeric value, the higher the priority of the path. This applies when the port is the root port.

Use this command for RSTP, STP or MSTP. When MSTP mode is configured, this will apply to the port's path cost for the CIST.

**Syntax** spanning-tree path-cost *<pathcost>*  
no spanning-tree path-cost

| Parameter               | Description                                                     |
|-------------------------|-----------------------------------------------------------------|
| <i>&lt;pathcost&gt;</i> | <i>&lt;1-200000000&gt;</i> The cost to be assigned to the port. |

**Default** The default path cost values and the range of recommended path cost values depend on the port speed, as shown in the following table from the IEEE 802.1q-2003 and IEEE 802.1d-2004 standards.

| Port speed         | Default path cost | Recommended path cost range |
|--------------------|-------------------|-----------------------------|
| Less than 100 Kb/s | 200,000,000       | 20,000,000-200,000,000      |
| 1Mbps              | 20,000,000        | 2,000,000-20,000,000        |
| 10Mbps             | 2,000,000         | 200,000-2,000,000           |
| 100 Mbps           | 200,000           | 20,000-200,000              |
| 1 Gbps             | 20,000            | 2,000-20,000                |
| 10 Gbps            | 2,000             | 200-2,000                   |
| 100 Gbps           | 200               | 20-200                      |
| 1Tbps              | 20                | 2-200                       |
| 10 Tbps            | 2                 | 2-20                        |

**Mode** Interface Configuration mode for switch port interface only.

**Example** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# spanning-tree path-cost 123

# spanning-tree portfast (STP)

**Overview** Use this command in Interface Configuration mode for a switch port interface only to set a port as an edge-port. The portfast feature enables a port to rapidly move to the forwarding state, without having first to pass through the intermediate spanning tree states. This command has the same effect as the [spanning-tree edgeport \(RSTP and MSTP\)](#) command, but the configuration displays differently in the output of some show commands.

**NOTE:** You can run either of two additional parameters with this command. To simplify the syntax these are documented as separate commands. See the following additional portfast commands:

- [spanning-tree portfast bpdu-filter](#) command
- [spanning-tree portfast bpdu-guard](#) command.

You can obtain the same effect by running the [spanning-tree edgeport \(RSTP and MSTP\)](#) command. However, the configuration output may display differently in some show commands.

Use the **no** variant of this command to set a port to its default state (not an edge-port).

**Syntax** `spanning-tree portfast`  
`no spanning-tree portfast`

**Default** Not an edge port.

**Mode** Interface Configuration mode for a switch port interface only.

**Usage** Portfast makes a port move from a blocking state to a forwarding state, bypassing both listening and learning states. The portfast feature is meant to be used for ports connected to end-user devices. Enabling portfast on ports that are connected to a workstation or server allows devices to connect to the network without waiting for spanning-tree to converge.

For example, you may need hosts to receive a DHCP address quickly and waiting for STP to converge would cause the DHCP request to time out. Ensure you do not use portfast on any ports connected to another device to avoid creating a spanning-tree loop on the network.

Use this command on a switch port that connects to a LAN with no other bridges attached. An edge port should never receive BPDUs. Therefore if an edge port receives a BPDU, the portfast feature takes one of three actions.

- Cease to act as an edge port and pass BPDUs as a member of a spanning tree network ([spanning-tree portfast \(STP\)](#) command disabled).
- Filter out the BPDUs and pass only the data and continue to act as a edge port ([spanning-tree portfast bpdu-filter](#) command enabled).
- Block the port to all BPDUs and data ([spanning-tree portfast bpdu-guard](#) command enabled).

**Example**    `awplus# configure terminal`  
              `awplus(config)# interface port1.0.2`  
              `awplus(config-if)# spanning-tree portfast`

**Related  
Commands**    `spanning-tree edgeport (RSTP and MSTP)`  
                  `show spanning-tree`  
                  `spanning-tree portfast bpdu-filter`  
                  `spanning-tree portfast bpdu-guard`

# spanning-tree portfast bpdu-filter

**Overview** This command sets the bpdu-filter feature and applies a filter to any BPDUs (Bridge Protocol Data Units) received. Enabling this feature ensures that configured ports will not transmit any BPDUs and will ignore (filter out) any BPDUs received. BPDU Filter is not enabled on a port by default.

Using the **no** variant of this command to turn off the bpdu-filter, but retain the port's status as an enabled port. If the port then receives a BPDU it will change its role from an **edge-port** to a **non edge-port**.

**Syntax (Global Configuration)** spanning-tree portfast bpdu-filter  
no spanning-tree portfast bpdu-filter

**Syntax (Interface Configuration)** spanning-tree portfast bpdu-filter {default|disable|enable}  
no spanning-tree portfast bpdu-filter

| Parameter   | Description                                                                                                                                                                               |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bpdu-filter | A port that has bpdu-filter enabled will not transmit any BPDUs and will ignore any BPDUs received. This port type has one of the following parameters (in Interface Configuration mode): |
| default     | Takes the setting that has been configured for the whole device, i.e. the setting made from the Global configuration mode.                                                                |
| disable     | Turns off BPDU filter.                                                                                                                                                                    |
| enable      | Turns on BPDU filter.                                                                                                                                                                     |

**Default** BPDU Filter is not enabled on any ports by default.

**Mode** Global Configuration and Interface Configuration

**Usage** This command filters the BPDUs and passes only data to continue to act as an edge port. Using this command in Global Configuration mode applies the portfast bpdu-filter feature to all ports on the device. Using it in Interface mode applies the feature to a specific port, or range of ports. The command will operate in both RSTP and MSTP networks.

Use the [show spanning-tree](#) command to display status of the bpdu-filter parameter for the switch ports.

**Example** To enable STP BPDU filtering in Global Configuration mode, enter the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-filter
```

To enable STP BPDU filtering in Interface Configuration mode, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast bpdu-filter enable
```

**Related  
Commands**

[spanning-tree edgeport \(RSTP and MSTP\)](#)  
[show spanning-tree](#)  
[spanning-tree portfast \(STP\)](#)  
[spanning-tree portfast bpdu-guard](#)

# spanning-tree portfast bpdu-guard

**Overview** This command applies a BPDU (Bridge Protocol Data Unit) guard to the port. A port with the bpdu-guard feature enabled will block all traffic (BPDUs and user data), if it starts receiving BPDUs.

Use this command in Global Configuration mode to apply BPDU guard to all ports on the device. Use this command in Interface mode for an individual interface or a range of interfaces specified. BPDU Guard is not enabled on a port by default.

Use the **no** variant of this command to disable the BPDU Guard feature on a device in Global Configuration mode or to disable the BPDU Guard feature on a port in Interface mode.

**Syntax (Global Configuration)** spanning-tree portfast bpdu-guard  
no spanning-tree portfast bpdu-guard

**Syntax (Interface Configuration)** spanning-tree portfast bpdu-guard {default|disable|enable}  
no spanning-tree portfast bpdu-guard

| Parameter  | Description                                                                                                                                                                         |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bpdu-guard | A port that has bpdu-guard turned on will enter the STP blocking state if it receives a BPDU. This port type has one of the following parameters (in Interface Configuration mode): |
| default    | Takes the setting that has been configured for the whole device, i.e. the setting made from the Global configuration mode.                                                          |
| disable    | Turns off BPDU guard.                                                                                                                                                               |
| enable     | Turns on BPDU guard and will also set the port as an edge port.                                                                                                                     |

**Default** BPDU Guard is not enabled on any ports by default.

**Mode** Global Configuration or Interface Configuration

**Usage** This command blocks the port(s) to all devices and data when enabled. BPDU Guard is a port-security feature that changes how a portfast-enabled port behaves if it receives a BPDU. When **bpdu-guard** is set, then the port shuts down if it receives a BPDU. It does not process the BPDU as it is considered suspicious. When **bpdu-guard** is not set, then the port will negotiate spanning-tree with the device sending the BPDUs. By default, bpdu-guard is not enabled on a port.

You can configure a port disabled by the bpdu-guard to re-enable itself after a specific time interval. This interval is set with the [spanning-tree errdisable-timeout interval](#) command. If you do not use the **errdisable-timeout** feature, then you will need to manually re-enable the port by using the **no shutdown** command.

Use the [show spanning-tree](#) command to display the device and port configurations for the BPDU Guard feature. It shows both the administratively configured and currently running values of bpdu-guard.

**Example** To enable STP BPDU guard in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
```

```
awplus(config)# spanning-tree portfast bpdu-guard
```

To enable STP BPDU guard in Interface Configuration mode, enter the below commands:

```
awplus# configure terminal
```

```
awplus(config)# interface port1.0.2
```

```
awplus(config-if)# spanning-tree portfast bpdu-guard enable
```

**Related Commands**

- [spanning-tree edgeport \(RSTP and MSTP\)](#)
- [show spanning-tree](#)
- [spanning-tree portfast \(STP\)](#)
- [spanning-tree portfast bpdu-filter](#)



# spanning-tree priority (bridge priority)

- Overview** Use this command to set the bridge priority for the device. A lower priority value indicates a greater likelihood of the device becoming the root bridge.
- Use this command for RSTP, STP or MSTP. When MSTP mode is configured, this will apply to the CIST.
- Use the **no** variant of this command to reset it to the default.

- Syntax** spanning-tree priority *<priority>*  
no spanning-tree priority

| Parameter               | Description                                                                              |
|-------------------------|------------------------------------------------------------------------------------------|
| <i>&lt;priority&gt;</i> | <i>&lt;0-61440&gt;</i> The bridge priority, which will be rounded to a multiple of 4096. |

- Default** The default priority is 32678.

- Mode** Global Configuration

- Usage** To force a particular device to become the root bridge use a lower value than other devices in the spanning tree.

- Example** awplus# configure terminal  
awplus(config)# spanning-tree priority 4096

- Related Commands** spanning-tree mst instance priority  
show spanning-tree

# spanning-tree priority (port priority)

**Overview** Use this command in Interface Configuration mode for a switch port interface only to set the port priority for port. A lower priority value indicates a greater likelihood of the port becoming part of the active topology.

Use this command for RSTP, STP, or MSTP. When the device is in MSTP mode, this will apply to the CIST.

Use the **no** variant of this command to reset it to the default.

**Syntax** spanning-tree priority *<priority>*  
no spanning-tree priority

| Parameter               | Description                                                                                      |
|-------------------------|--------------------------------------------------------------------------------------------------|
| <i>&lt;priority&gt;</i> | <0-240>, in increments of 16. The port priority, which will be rounded down to a multiple of 16. |

**Default** The default priority is 128.

**Mode** Interface Configuration mode for a switch port interface only.

**Usage** To force a port to be part of the active topology (for instance, become the root port or a designated port) use a lower value than other ports on the device. (This behavior is subject to network topology, and more significant factors, such as bridge ID.)

**Example** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# spanning-tree priority 16

**Related Commands** spanning-tree mst instance priority  
spanning-tree priority (bridge priority)  
show spanning-tree

# spanning-tree restricted-role

**Overview** Use this command in Interface Configuration mode for a switch port interface only to restrict the port from becoming a root port.

Use the **no** variant of this command to disable the restricted role functionality.

**Syntax** spanning-tree restricted-role  
no spanning-tree restricted-role

**Default** The restricted role is disabled.

**Mode** Interface Configuration mode for a switch port interface only.

**Example** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# spanning-tree restricted-role

## spanning-tree restricted-tcn

**Overview** Use this command in Interface Configuration mode for a switch port interface only to prevent TCN (Topology Change Notification) BPDUs (Bridge Protocol Data Units) from being sent on a port. If this command is enabled, after a topology change a bridge is prevented from sending a TCN to its designated bridge.

Use the **no** variant of this command to disable the restricted TCN functionality.

**Syntax** spanning-tree restricted-tcn  
no spanning-tree restricted-tcn

**Default** The restricted TCN is disabled.

**Mode** Interface Configuration mode for a switch port interface only.

**Example** awplus# configure terminal  
awplus(config)# interface port1.0.2  
awplus(config-if)# spanning-tree restricted-tcn

# spanning-tree transmit-holdcount

**Overview** Use this command to set the maximum number of BPDU transmissions that are held back.

Use the **no** variant of this command to restore the default transmit hold-count value.

**Syntax** spanning-tree transmit-holdcount  
no spanning-tree transmit-holdcount

**Default** Transmit hold-count default is 3.

**Mode** Global Configuration

**Example** awplus# configure terminal  
awplus(config)# spanning-tree transmit-holdcount

# undebg mstp

**Overview** This command applies the functionality of the no `debug mstp` (RSTP and STP) command.

# 13

# Link Aggregation Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure a static channel group (static aggregator) and dynamic channel group (LACP channel group, etherchannel or LACP aggregator). Link aggregation is also sometimes referred to as channeling.

**NOTE:** *AlliedWare Plus™ supports IEEE 802.3ad link aggregation and uses the Link Aggregation Control Protocol (LACP). LACP does not interoperate with devices that use Port Aggregation Protocol (PAgP).*

*Link aggregation does not necessarily achieve exact load balancing across the links. The load sharing algorithm is designed to ensure that any given data flow always goes down the same link. It also aims to spread data flows across the links as evenly as possible.*

*For example, for a 2 Gbps LAG that is a combination of two 1 Gbps ports, any one flow of traffic can only ever reach a maximum throughput of 1 Gbps. However, the hashing algorithm should spread the flows across the links so that when many flows are operating, the full 2 Gbps can be utilized.*

For a description of static and dynamic link aggregation (LACP), and configuration examples, see the [Link Aggregation Feature Overview and Configuration Guide](#).

- Command List**
- [“channel-group”](#) on page 481
  - [“clear lacp counters”](#) on page 483
  - [“debug lacp”](#) on page 484
  - [“lacp port-priority”](#) on page 485
  - [“lacp system-priority”](#) on page 486
  - [“lacp timeout”](#) on page 487
  - [“show debugging lacp”](#) on page 489
  - [“show diagnostic channel-group”](#) on page 490
  - [“show etherchannel”](#) on page 491

- [“show etherchannel detail”](#) on page 492
- [“show etherchannel summary”](#) on page 493
- [“show lacp sys-id”](#) on page 494
- [“show lacp-counter”](#) on page 495
- [“show port etherchannel”](#) on page 496
- [“show static-channel-group”](#) on page 498
- [“static-channel-group”](#) on page 499
- [“undebbug lacp”](#) on page 501



# channel-group

**Overview** Use this command to add the device port to a dynamic channel group specified by the dynamic channel group number, and set its mode. This command enables LACP link aggregation on the device port, so that it may be selected for aggregation by the local system. Dynamic channel groups are also known as LACP channel groups, LACP aggregators or etherchannels.

You can create up to 2 dynamic (LACP) channel groups (or up to 2 static channel groups).

Use the **no** variant of this command to turn off link aggregation on the device port. You will be returned to Global Configuration mode from Interface Configuration mode.

**Syntax** `channel-group <dynamic-channel-group-number> mode {active|passive}`  
`no channel-group`

| Parameter                                         | Description                                                                                                                                                                                 |
|---------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;dynamic-channel-group-number&gt;</code> | <1-2> Specify a dynamic channel group number for an LACP link.                                                                                                                              |
| <code>active</code>                               | Enables initiation of LACP negotiation on a port. The port will transmit LACP dialogue messages whether or not it receives them from the partner system.                                    |
| <code>passive</code>                              | Disables initiation of LACP negotiation on a port. The port will only transmit LACP dialogue messages if the partner systems is transmitting them, i.e., the partner is in the active mode. |

**Mode** Interface Configuration

**Usage** All the device ports in a channel-group must belong to the same VLANs, have the same tagging status, and can only be operated on as a group. All device ports within a channel group must have the same port speed and be in full duplex mode.

Once the LACP channel group has been created, it is treated as a device port, and can be referred to in most other commands that apply to device ports.

To refer to an LACP channel group in other LACP commands, use the channel group number. To specify an LACP channel group (LACP aggregator) in other commands, prefix the channel group number with **po**. For example, 'po2' refers to the LACP channel group with channel group number 2.

Link aggregation hashes the source and destination MAC address to select a link on which to send a packet. So packet flow between a pair of hosts always takes the same link inside the Link Aggregation Group (LAG). The net effect is that the bandwidth for a given packet stream is restricted to the speed of one link in the LAG. This hashing mechanism cannot be changed.

For more information about LACP, see the [Link Aggregation Feature Overview and Configuration Guide](#).

**Examples** To add device port1.0.6 to a newly created LACP channel group 2 use the commands below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# channel-group 2 mode active
```

To remove device port1.0.6 from any created LACP channel groups use the command below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no channel-group
awplus(config)#
```

To reference the pre-defined LACP channel group 2 as an interface, apply commands as below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# channel-group 2 mode active
awplus(config-if)# exit
awplus(config)# interface port.1.0.6
awplus(config-if)# channel-group 2 mode active
awplus(config-if)# exit
awplus(config)# interface po2
awplus(config-if)#
```

**Related Commands**

- [show etherchannel](#)
- [show etherchannel detail](#)
- [show etherchannel summary](#)
- [show port etherchannel](#)

# clear lacp counters

**Overview** Use this command to clear all counters of all present LACP aggregators (channel groups) or a given LACP aggregator.

**Syntax** `clear lacp [<1-2>] counters`

| Parameter | Description           |
|-----------|-----------------------|
| <1 - 2>   | Channel-group number. |

**Mode** Privileged Exec

**Example** `awplus# clear lacp 2 counters`

# debug lacp

**Overview** Use this command to enable all LACP troubleshooting functions.

Use the **no** variant of this command to disable this function.

**Syntax** `debug lacp {all|cli|event|ha|packet|sync|timer[detail]}`  
`no debug lacp {all|cli|event|ha|packet|sync|timer[detail]}`

| Parameter | Description                                                                                               |
|-----------|-----------------------------------------------------------------------------------------------------------|
| all       | Turn on all debugging for LACP.                                                                           |
| cli       | Specifies debugging for CLI messages.<br>Echoes commands to the console.                                  |
| event     | Specifies debugging for LACP events.<br>Echoes events to the console.                                     |
| ha        | Specifies debugging for HA (High Availability) events.<br>Echoes High Availability events to the console. |
| packet    | Specifies debugging for LACP packets.<br>Echoes packet contents to the console.                           |
| sync      | Specified debugging for LACP synchronization.<br>Echoes synchronization to the console.                   |
| timer     | Specifies debugging for LACP timer.<br>Echoes timer expiry to the console.                                |
| detail    | Optional parameter for LACP timer-detail.<br>Echoes timer start/stop details to the console.              |

**Mode** Privileged Exec and Global Configuration

**Examples** `awplus# debug lacp timer detail`  
`awplus# debug lacp all`

**Related Commands** [show debugging lacp](#)  
[undebug lacp](#)

# lacp port-priority

**Overview** Use this command to set the priority of a device port. Ports are selected for aggregation based on their priority, with the higher priority (numerically lower) ports selected first.

Use the **no** variant of this command to reset the priority of port to the default.

**Syntax** lacp port-priority <1-65535>  
no lacp port-priority

| Parameter   | Description                     |
|-------------|---------------------------------|
| <1 - 65535> | Specify the LACP port priority. |

**Default** The default is 32768.

**Mode** Interface Configuration

**Example** awplus# configure terminal  
awplus(config)# interface port1.0.5  
awplus(config-if)# lacp port-priority 34

# lacp system-priority

**Overview** Use this command to set the system priority of a local system. This is used in determining the system responsible for resolving conflicts in the choice of aggregation groups.

Use the **no** variant of this command to reset the system priority of the local system to the default.

**Syntax** lacp system-priority <1-65535>  
no lacp system-priority

| Parameter   | Description                                                          |
|-------------|----------------------------------------------------------------------|
| <1 - 65535> | LACP system priority. Lower numerical values have higher priorities. |

**Default** The default is 32768.

**Mode** Global Configuration

**Example** awplus# configure terminal  
awplus(config)# lacp system-priority 6700

# lacp timeout

**Overview** Use this command to set the short or long timeout on a port. Ports will time out of the aggregation if three consecutive updates are lost.

**Syntax** lacp timeout {short|long}

| Parameter | Description                                                            |
|-----------|------------------------------------------------------------------------|
| timeout   | Number of seconds before invalidating a received LACP data unit (DU).  |
| short     | LACP short timeout. The <b>short</b> timeout value is <b>1</b> second. |
| long      | LACP long timeout. The <b>long</b> timeout value is <b>30</b> seconds. |

**Default** The default is **long** timeout (30 seconds).

**Mode** Interface Configuration

**Usage** This command enables the device to indicate the rate at which it expects to receive LACPDU's from its neighbor.

If the timeout is set to **long**, then the device expects to receive an update every **30** seconds, and this will time a port out of the aggregation if no updates are seen for 90 seconds (i.e. 3 consecutive updates are lost).

If the timeout is set to **short**, then the device expects to receive an update every second, and this will time a port a port out of the aggregation if no updates are seen for 3 seconds (i.e. 3 consecutive updates are lost).

The device indicates its preference by means of the 'Timeout' field in the 'Actor' section of its LACPDU's. If the 'Timeout' field is set to 1, then the device has set the **short** timeout. If the 'Timeout' field is set to 0, then the device has set the **long** timeout.

Setting the **short** timeout enables the device to be more responsive to communication failure on a link, and does not add too much processing overhead to the device (1 packet per second).

**NOTE:** It is not possible to configure the rate that the device sends LACPDU's; the device must send at the rate which the neighbor indicates it expects to receive LACPDU's.

**Examples** The following commands set the LACP long timeout period for 30 seconds on port1.0.2.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lacp timeout long
```

The following commands set the LACP short timeout for 1 second on port1.0.2.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lacp timeout short
```



# show debugging lacp

**Overview** Use this command to display the LACP debugging option set.

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 debugging lacp

**Mode** User Exec and Privileged Exec

**Example** awplus# show debugging lacp

**Output** Figure 13-1: Example output from the **show debugging lacp** command

```
LACP debugging status:
LACP timer debugging is on
LACP timer-detail debugging is on
LACP cli debugging is on
LACP packet debugging is on
LACP event debugging is on
LACP sync debugging is on
```

**Related  
Commands** [debug lacp](#)

# show diagnostic channel-group

**Overview** This command displays dynamic and static channel group interface status information. The output of this command is useful for Allied Telesis authorized service personnel for diagnostic purposes.

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 diagnostic channel-group

**Mode** User Exec and Privileged Exec

**Example** awplus# show diagnostic channel-group

**Output** Figure 13-2: Example output from the **show diagnostic channel-group** command

```
awplus# show diagnostic channel-group

Channel Group Info based on NSM:
Note: Pos - position in hardware table

Dev Interface IfIndex Member port IfIndex Active Pos

 po1 4601 port1.0.4 5004 No
 po1 4601 port1.0.5 5005 No

Channel Group Info based on HSL:
Note: Pos - position in hardware table

Dev Interface IfIndex Member port IfIndex Active Pos

 po1 4601 N/a

Channel Group Info based on IPIFWD:
Note: Pos - position in hardware table

Dev Interface IfIndex Member port IfIndex Active Pos

 po1 4601 N/a

No error found
```

**Related Commands** [show tech-support](#)

# show etherchannel

**Overview** Use this command to display information about a LACP channel specified by the channel group number.

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 etherchannel [<1-2>]

| Parameter | Description           |
|-----------|-----------------------|
| <1-2>     | Channel-group number. |

**Mode** User Exec and Privileged Exec

**Example** awplus# show etherchannel 2

**Output** Figure 13-3: Example output from the **show etherchannel** command

```
awplus#show etherchannel
% LAG Maximum : 4
% LAG Static Maximum: 2
% LAG Dynamic Maximum: 2
% LAG Static Count : 0
% LAG Dynamic Count : 1
% LAG Total Count : 1
% LACP Aggregator: po1
% Member:
 port1.0.5
 port1.0.6
```

Figure 13-4: Example output from the **show etherchannel** command for a particular channel

```
awplus#show etherchannel 1
Aggregator po1 (4601)
Mac address: 00:00:00:00:00:00
Admin Key: 0001 - Oper Key 0000
Receive link count: 0 - Transmit link count: 0
Individual: 0 - Ready: 0
Partner LAG: 0x0000,00-00-00-00-00
Link: port1.0.5 (5005) disabled
Link: port1.0.6 (5006) disabled
```

# show etherchannel detail

**Overview** Use this command to display detailed information about all LACP channels.  
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 etherchannel detail

**Mode** User Exec and Privileged Exec

**Example** awplus# show etherchannel detail

**Output** Figure 13-5: Example output from the **show etherchannel detail** command

```
Aggregator po1 (IfIndex: 4501)
 Mac address: 00:00:cd:24:fd:29
 Admin Key: 0001 - Oper Key 0001
 Receive link count: 1 - Transmit link count: 0
 Individual: 0 - Ready: 1
 Partner LAG: 0x8000,00-00-cd-24-da-a7
 Link: port1.0.1 (IfIndex: 5001) disabled
 Link: port1.0.2 (IfIndex: 5002) sync: 1
Aggregator po2 (IfIndex: 4502)
 Mac address: 00:00:cd:24:fd:29
 Admin Key: 0002 - Oper Key 0002
 Receive link count: 1 - Transmit link count: 0
 Individual: 0 - Ready: 1
 Partner LAG: 0x8000,00-00-cd-24-da-a7
 Link: port1.0.6 (IfIndex: 5007) disabled
```

# show etherchannel summary

**Overview** Use this command to display a summary of all LACP channels.

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 etherchannel summary

**Mode** User Exec and Privileged Exec

**Example** awplus# show etherchannel summary

**Output** Figure 13-6: Example output from the **show etherchannel** summary command

```
% Aggregator po1
% Admin Key: 0001 - Oper Key 0001
% Link: port1.0.1 (5001) disabled
% Link: port1.0.2 (5002) sync: 1
% Aggregator po2
% Admin Key: 0002 - Oper Key 0002
% Link: port1.0.6 (5007) disabled
```

# show lacp sys-id

**Overview** Use this command to display the LACP system ID and priority.

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 lacp sys-id

**Mode** User Exec and Privileged Exec

**Example** awplus# show lacp sys-id

**Output** Figure 13-7: Example output from the **show lacp sys-id** command

```
System Priority: 0x8000 (32768)
MAC Address: 0200.0034.5684
```

# show lacp-counter

**Overview** Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

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 lacp-counter [<1-2>]
```

| Parameter | Description           |
|-----------|-----------------------|
| <1-2>     | Channel-group number. |

**Mode** User Exec and Privileged Exec

**Example** awplus# show lacp-counter 2

**Output** Figure 13-8: Example output from the **show lacp-counter** command

|                                  |         |      |        |      |          |      |
|----------------------------------|---------|------|--------|------|----------|------|
| % Traffic statistics             |         |      |        |      |          |      |
| Port                             | LACPDUs |      | Marker |      | Pckt err |      |
|                                  | Sent    | Recv | Sent   | Recv | Sent     | Recv |
| % Aggregator po2 (IfIndex: 4604) |         |      |        |      |          |      |
| port1.0.2                        | 0       | 0    | 0      | 0    | 0        | 0    |

# show port etherchannel

**Overview** Use this command to show LACP details of the device port specified.

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 port etherchannel <port>

| Parameter | Description                                                |
|-----------|------------------------------------------------------------|
| <port>    | Name of the device port to display LACP information about. |

**Mode** User Exec and Privileged Exec

**Example** awplus# show port etherchannel port1.0.1

**Output** Figure 13-9: Example output from the **show port etherchannel** command



Link:  
port1.0.1 (5001)

Aggregator: po1 (4501)

Receive machine state: Current

Periodic Transmission machine state: Fast periodic

Mux machine state: Collecting/Distributing

Actor Information:

Partner Information:

|                          |          |                            |                   |
|--------------------------|----------|----------------------------|-------------------|
| Selected .....           | Selected | Partner Sys Priority ..... | 0                 |
| Physical Admin Key ..... | 1        | Partner System ..          | 00-00-00-00-00-00 |
| Port Key .....           | 5        | Port Key .....             | 0                 |
| Port Priority .....      | 32768    | Port Priority .....        | 0                 |
| Port Number .....        | 5001     | Port Number .....          | 0                 |
| Mode .....               | Active   | Mode .....                 | Passive           |
| Timeout .....            | Long     | Timeout .....              | Short             |
| Individual .....         | Yes      | Individual .....           | Yes               |
| Synchronised .....       | Yes      | Synchronised .....         | Yes               |
| Collecting .....         | Yes      | Collecting .....           | Yes               |
| Distributing .....       | Yes      | Distributing .....         | Yes               |
| Defaulted .....          | Yes      | Defaulted .....            | Yes               |
| Expired .....            | No       | Expired .....              | No                |

# show static-channel-group

**Overview** Use this command to display all configured static channel groups and their corresponding member ports. Note that a static channel group is the same as a static aggregator.

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 static-channel-group

**Mode** User Exec and Privileged Exec

**Example** awplus# show static-channel-group

**Output** Figure 13-10: Example output from the **show static-channel-group** command

```
awplus#show static-channel-group
% LAG Maximum : 2
% LAG Static Maximum: 2
% LAG Dynamic Maximum: 2
% LAG Static Count : 0
% LAG Dynamic Count : 1
% LAG Total Count : 1
```

**Related Commands** [static-channel-group](#)

# static-channel-group

**Overview** Use this command to create a static channel group, also known as a static aggregator, or add a member port to an existing static channel group.

You can create up to 2 static channel groups (or up to 2 dynamic channel groups).

Use the **no** variant of this command to remove the device port from the static channel group.

**Syntax** static-channel-group <static-channel-group-number>  
no static-channel-group

| Parameter                     | Description                        |
|-------------------------------|------------------------------------|
| <static-channel-group-number> | <1-2> Static channel group number. |

**Mode** Interface Configuration

**Usage** This command adds the device port to the static channel group with the specified channel group number. If the channel group does not exist, it is created, and the port is added to it. The **no** prefix detaches the port from the static channel group. If the port is the last member to be removed, the static channel group is deleted.

All the ports in a channel group must have the same VLAN configuration: they must belong to the same VLANs and have the same tagging status, and can only be operated on as a group.

Once the static channel group has been created, it is treated as a device port, and can be referred to in other commands that apply to device ports.

To refer to a static channel group in other static channel group commands, use the channel group number. To specify a static channel group in other commands, prefix the channel group number with **sa**. For example, 'sa2' refers to the static channel group with channel group number 2.

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](#).

**Examples** To define a static channel group on a device port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# static-channel-group 2
```

To reference the pre-defined static channel group 2 as an interface apply the example commands as below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface port.1.0.8
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)#
```

**Related  
Commands** [show static-channel-group](#)

# undebbug lacp

**Overview** This command applies the functionality of the no [debug lacp](#) command.

# 14

# Power over Ethernet Commands

## Introduction

**Overview** This chapter contains an alphabetical list of commands used to configure Power over Ethernet (PoE). Each command contains a functional description and shows examples of configuration and output screens for show commands. These commands are only supported on PoE capable ports. An error message will display on the console if you enter a PoE command on a port that does not support PoE. The following documents offer further information for configuring PoE on AlliedWare Plus switches.

- the [PoE Feature Overview and Configuration Guide](#).
- the [SNMP MIBs Overview](#), for information about which PoE MIB objects are supported.
- the [SNMP Feature Overview and Configuration Guide](#), for information about SNMP traps.

Power over Ethernet (PoE) is a technology allowing devices such as IP phones to receive power over existing LAN cabling.

PoE is configured using the commands in this chapter. Note the Power Sourcing Equipment (PSE) referred to throughout this chapter is an Allied Telesis PoE switch running the AlliedWare Plus™ Operating System, supporting the IEEE 802.3af and IEEE 802.3at Power Ethernet standards. The Powered Device (PD) referred to throughout this chapter is a PoE or PoE+ powered device, such as an IP phone or a Wireless Access Point (WAP).

**NOTE:**

- Command List**
- [“clear power-inline counters interface”](#) on page 504
  - [“debug power-inline”](#) on page 505
  - [“power-inline allow-legacy”](#) on page 507
  - [“power-inline description”](#) on page 508
  - [“power-inline enable”](#) on page 509

- [“power-inline max”](#) on page 510
- [“power-inline priority”](#) on page 512
- [“power-inline usage-threshold”](#) on page 514
- [“service power-inline”](#) on page 515
- [“show debugging power-inline”](#) on page 516
- [“show power-inline”](#) on page 517
- [“show power-inline counters”](#) on page 519
- [“show power-inline interface”](#) on page 521
- [“show power-inline interface detail”](#) on page 523

# clear power-inline counters interface

**Overview** This command will clear the counters from a specified port, a range of ports, or all ports on the Power Sourcing Equipment (PSE). If no ports are entered then PoE counters for all ports are cleared. It will also clear all Power over Ethernet (PoE) counters supported by the Power Ethernet MIB (RFC 3621).

**Syntax** clear power-inline counters interface [*<port-list>*]

| Parameter                | Description                                                 |
|--------------------------|-------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | Selects the port or ports whose counters are to be cleared. |

**Mode** Privileged Exec

**Usage** The PoE counters are displayed with the [show power-inline counters](#) command.

**Examples** To clear the PoE counters for port `t1.0.2` only, use the following command:

```
awplus# clear power-inline counters interface port1.0.2
```

To clear the PoE counters for all ports, use the following command:

```
awplus# clear power-inline counters interface
```

**Validation Commands** [show power-inline counters](#)



# debug power-inline

**Overview** This command enables debugging display for messages that are specific to Power over Ethernet (PoE).

Use the **no** variant of this command to disable the specified PoE debugging messages.

**Syntax** debug power-inline [all|event|info|power]  
no debug power-inline [all|event|info|power]

| Parameter | Description                                                                                                                      |
|-----------|----------------------------------------------------------------------------------------------------------------------------------|
| all       | Displays all (event, info, nsm, power) debug messages.                                                                           |
| event     | Displays event debug information, showing any error conditions that may occur during PoE operation.                              |
| info      | Displays informational level debug information, showing high-level essential debugging, such as information about message types. |
| power     | Displays power management debug information.                                                                                     |

**Default** No debug messages are enabled by default.

**Mode** Privileged Exec

**Usage** Use the [terminal monitor](#) command to display PoE debug messages on the console.

Use the [show debugging power-inline](#) command to show the PoE debug configuration.

**Examples** To enable PoE debugging and start the display of PoE event and info debug messages on the console, use the following commands:

```
awplus# terminal monitor
awplus# debug power-inline event info
```

To enable PoE debugging and start the display of all PoE debugging messages on the console, use the following commands:

```
awplus# terminal monitor
awplus# debug power-inline all
```

To disable PoE debugging and stop the display of PoE event and info debug messages on the console, use the following command:

```
awplus# no debug power-inline event info
```

To disable all PoE debugging and stop the display of any PoE debugging messages on the console, use the following command:

```
awplus# no debug power-inline all
```

**Validation** [show debugging power-inline](#)  
**Commands**

**Related** [terminal monitor](#)  
**Commands**

# power-inline allow-legacy

**Overview** This command enables detection of pre-IEEE 802.3af Power Ethernet standard legacy Powered Devices (PDs).

The no variant of this command disables detection of pre-IEEE 802.3af Power Ethernet standard legacy Powered Devices (PDs).

**Syntax** power-inline allow-legacy  
no power-inline allow-legacy

**Default** Detection of legacy PDs is enabled on all ports on the Power Sourcing Equipment (PSE).

**Mode** Global Configuration

**Examples** To disable detection of legacy PDs, use the following commands:

```
awplus# configure terminal
awplus(config)# no power-inline allow-legacy
```

To enable detection of legacy PDs, use the following commands:

```
awplus# configure terminal
awplus(config)# power-inline allow-legacy
```

**Validation Commands** show power-inline  
show running-config power-inline

# power-inline description

**Overview** This command adds a description for a Powered Device (PD) connected to a PoE port.

The **no** variant of this command clears a previously entered description for a connected PD, resetting the PD description to the default (null).

**Syntax** power-inline description *<pd-description>*  
no power-inline description

| Parameter                     | Description                                                                                                             |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;pd-description&gt;</i> | Description of the PD connected to the PoE capable port (with a maximum 256 character string limit per PD description). |

**Default** No description for a connected PD is set by default.

**Mode** Interface Configuration

**Usage** Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding [interface \(to configure\)](#) command. If you specify a range or list of ports they must all be PoE capable ports.

**Examples** To add the description Desk Phone for a connected PD on port `t1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline description Desk Phone
```

To clear the description as added above for the connected PD on port `t1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline description
```

**Validation Commands** [show power-inline interface](#)  
[show running-config power-inline](#)

# power-inline enable

**Overview** This command enables Power over Ethernet (PoE) to detect a connected Powered Device (PD) and supply power from the Power Sourcing Equipment (PSE).

The **no** variant of this command disables PoE functionality on the selected PoE port(s). No power is supplied to a connected PD after PoE is disabled on the selected PoE port(s).

**Syntax** power-inline enable  
no power-inline enable

**Default** PoE is enabled by default on all ports on the PSE.

**Mode** Interface Configuration

**Usage** Select a PoE port, a list of PoE ports, or a range of PoE ports from the preceding [interface \(to configure\)](#) command. If you specify a range or list of ports they must all be PoE capable ports.

No PoE log messages are generated for specified PoE port(s) after PoE is disabled. The disabled PoE port(s) still provide Ethernet connectivity after PoE is disabled.

**Examples** To disable PoE on ports port1.0.1 to port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# no power-inline enable
```

To enable PoE on ports port1.0.1 to port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# power-inline enable
```

**Validation Commands** [show power-inline](#)  
[show power-inline interface](#)  
[show power-inline interface detail](#)  
[show running-config power-inline](#)

# power-inline max

**Overview** This command sets the “maximum” power allocated to a Power over an Ethernet (PoE and PoE+) port. The amount of power actually supplied to the port depends on the power requirements of the connected PD. It is also a function of the total PoE power loading on the switch and the PoE priority set for the port by the [power-inline priority](#) command. However this command (power-inline max) does apply a “maximum” value to the power that the port is able to supply.

The IE200-6 Series switches are able to supply 802.3at (PoE+) power levels to all their PoE-capable ports. This command controls the power output for each port, however this should not be necessary on an IE200-6 Series switch.

Note that the value set by this command will be the figure the switch will use when apportioning the power budget for its ports. For example, if 15.4 W is assigned to a port whose PD only consumes 5 W, the switch will reserve the full 15.4 W for this port when determining its total power PoE power requirement.

The **no** variant of this command sets the maximum power supplied to a PoE port to the default, which is set to the maximum power limit for the class of the connected Powered Device (PD).

**Syntax** power-inline max <4000-30000>  
no power-inline max

| Parameter    | Description                                                   |
|--------------|---------------------------------------------------------------|
| <4000-30000> | The maximum power allocated to a PoE port in milliwatts (mW). |

**Default** The Power Sourcing Equipment (PSE) supplies the maximum power limit for the class of the PD connected to the port by default.

**NOTE:** See the [PoE Feature Overview and Configuration Guide](#) for further information about power classes.

**Mode** Interface Configuration

**Usage** Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding [interface \(to configure\)](#) command. If you specify a range or list of ports they must all be PoE capable ports.

If you select a range of PoE ports in Interface Configuration mode before issuing this command, then each port in the range selected will have the same maximum power value configured. If the PoE port attempts to draw more than the maximum power, this is logged and all power is removed. Note that the value entered is rounded up to the next value supported by the hardware.

See the actual value used, as shown after command entry, in the sample console output below:

```
awplus#configure terminal
awplus(config)#interface
port1.0.1
awplus(config-if)#power-line max 5300
% The maximum power has been rounded to 5450mW in hardware.
```

See the [LLDP Feature Overview and Configuration Guide](#) for information about power monitoring at the PD.

Note the difference in power supplied from the PSE to the power available at the PD due to line loss.

See the [PoE Feature Overview and Configuration Guide](#) for further information about the difference between the power supplied from the PSE and the power available at the PD.

**Examples** To set the maximum power supplied to ports in the range 1.0.2 to 1.0.4 to 6450mW per port, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# power-inline max 6450
```

To set the maximum power supplied to port 1.0.2, to 6450 mW, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline max 6450
```

To clear the user-configured maximum power supplied to port 1.0.2, and revert to using the default maximum power of 30000 mW, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline max
```

**Validation Commands** [show power-inline interface](#)  
[show running-config power-inline](#)

# power-inline priority

**Overview** This command sets the Power over Ethernet (PoE) priority level of a PoE port to one of three available priority levels:

- low
- high
- critical

The IE200-6 Series switches are able to supply 802.3at (PoE+) power levels to all their PoE-capable ports. This command prioritizes ports if necessary, however this should not be necessary on an IE200-6 Series switch.

The **no** variant of this command restores the PoE port priority to the default (low).

**Syntax** power-inline priority {low|high|critical}  
no power-inline priority

| Parameter | Description                                                                                                                                                                                                                                                       |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| low       | The lowest priority for a PoE enabled port (default). PoE ports set to low only receive power if all the PoE ports assigned to the other two levels are already receiving power.                                                                                  |
| high      | The second highest priority for a PoE enabled port. PoE ports set to high receive power only if all the ports set to critical are already receiving power.                                                                                                        |
| critical  | The highest priority for a PoE enabled port. PoE ports set to critical are guaranteed power before any ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only if all Critical ports are receiving power. |

**Default** The default priority is low for all PoE ports on the Power Sourcing Equipment (PSE).

**Mode** Interface Configuration

**Usage** Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding [interface \(to configure\)](#) command. If you specify a range or list of ports they must all be PoE capable ports.

PoE ports with higher priorities are given power before PoE ports with lower priorities. If the priorities for two PoE ports are the same then the lower numbered PoE port is given power before the higher numbered PoE port.

See the [PoE Feature Overview and Configuration Guide](#) for further information about PoE priority.



**Examples** To set the priority level to high for port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline priority high
```

To reset the priority level to the default for port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline priority
```

**Validation  
Commands** [show power-inline](#)  
[show power-inline interface](#)  
[show running-config power-inline](#)

**Related  
Commands** [power-inline usage-threshold](#)

# power-inline usage-threshold

**Overview** This command sets the level at which the Power Sourcing Equipment (PSE) will issue a message that the power supplied to all Powered Devices (PDs) has reached a critical level of the nominal power rating for the PSE. The level is set as a percentage of total available power.

The **no** variant of this command resets the notification usage-threshold to the default (80% of the nominal power rating of the PSE).

**Syntax** power-inline usage-threshold <1-99>  
no power-inline usage-threshold

| Parameter | Description                                                  |
|-----------|--------------------------------------------------------------|
| <1-99>    | The usage-threshold percentage configured with this command. |

**Default** The default power usage threshold is 80% of the nominal power rating of the PSE.

**Mode** Global Configuration

**Usage** Use the [snmp-server enable trap](#) command to configure SNMP notification. An SNMP notification is sent when the usage-threshold, as configured in the example, is exceeded.

**Examples** To generate SNMP notifications when power supplied exceeds 70% of the nominal PSE power, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap power-inline
awplus(config)# power-inline usage-threshold 70
```

To reset the notification threshold to the default (80% of the nominal PSE power rating), use the following commands:

```
awplus# configure terminal
awplus(config)# no power-inline usage-threshold
```

**Validation Commands** [show power-inline interface](#)  
[show running-config power-inline](#)

**Related Commands** [snmp-server enable trap](#)

# service power-inline

**Overview** This command enables Power over Ethernet (PoE) globally on the Power Sourcing Equipment (PSE) for all PoE ports.

**Syntax** service power-inline  
no service power-inline

**Default** PoE functionality is enabled by default on the PSE.

**Mode** Global Configuration

**Examples** To disable PoE on the PSE, use the following commands:

```
awplus# configure terminal
awplus(config)# no service power-inline
```

To re-enable PoE on the PSE, if PoE has been disabled, use the following commands:

```
awplus# configure terminal
awplus(config)# service power-inline
```

**Validation** show power-inline  
**Commands** show running-config power-inline

# show debugging power-inline

**Overview** This command displays Power over Ethernet (PoE) debug settings.  
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 debugging power-inline

**Mode** User Exec and Privileged Exec

**Example** To display PoE debug settings, use the following command:

```
awplus# show debugging power-inline
```

**Output** Figure 14-1: Example output from the **show debugging power-inline** command

```
awplus#show debugging power-inline
PoE Debugging status:
PoE Informational debugging is disabled
PoE Event debugging is disabled
PoE Power Management debugging is disabled

PoE NSM debugging is enabled
```

**Related Commands** [debug power-inline](#)  
[terminal monitor](#)

# show power-inline

**Overview** This command displays the Power over Ethernet (PoE) status for all ports on the Power Sourcing Equipment (PSE).

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 power-inline

**Mode** User Exec and Privileged Exec

**Example** To display the PoE status for all ports on the PSE, use the following command:

```
awplus# show power-inline
```

Table 14-1: Parameters in the **show power-inline** command output

| Parameter                 | Description                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nominal Power             | The nominal power available on the switch in watts (W).                                                                                                                                                                                                                                                                                                                                                            |
| Power Allocated           | The current power allocated in watts (W) that is available to be drawn by any connected Powered Devices (PDs). This is updated every 5 seconds.                                                                                                                                                                                                                                                                    |
| Actual Power Consumption  | The current power consumption in watts (W) drawn by all connected Powered Devices (PDs). This is updated every 5 seconds.                                                                                                                                                                                                                                                                                          |
| Operational Status        | The operational status of the PSU hardware on the PSE when this command was issued: <ul style="list-style-type: none"><li>• <b>On</b> if the PSU as installed inside the PSE is switched on.</li><li>• <b>Off</b> when the PSU in the PSE is switched off (an RPS may be connected to the PSE to power PoE instead of the PSU).</li><li>• <b>Fault</b> when there is an issue with the PSE PSU hardware.</li></ul> |
| Power Usage Threshold (%) | The configured SNMP trap / log threshold for the PSE, as configured from a <a href="#">power-inline usage-threshold</a> command.                                                                                                                                                                                                                                                                                   |
| Interface                 | The PoE port(s) in the format port x . y . z, where x is the device number, y is the module number within the device, and z is the PoE port number within the module.                                                                                                                                                                                                                                              |
| Admin                     | The administrative state of PoE on a PoE port, either <b>Enabled</b> or <b>Disabled</b> .                                                                                                                                                                                                                                                                                                                          |

Table 14-1: Parameters in the **show power-inline** command output (cont.)

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pri       | <p>The current PoE priorities for PoE ports on the PSE, as configured from a <a href="#">power-inline priority</a> command:</p> <ul style="list-style-type: none"> <li>• <b>Low</b> displays when the low parameter is issued. The lowest priority for a PoE enabled port (default).</li> <li>• <b>High</b> displays when the high parameter is issued. The second highest priority for a PoE enabled port.</li> <li>• <b>Crit</b> displays when the critical parameter is issued. The highest priority for a PoE enabled port.</li> </ul> |
| Oper      | <p>The current PSE PoE port state when this command was issued:</p> <ul style="list-style-type: none"> <li>• <b>Powered</b> displays when there is a PD connected and power is being supplied from the PSE.</li> <li>• <b>Disabled</b> displays when supplying power would make the PSE go over the power budget.</li> <li>• <b>Off</b> displays when PoE has been disabled for the PoE port.</li> <li>• <b>Fault</b> displays when a PSE goes over its power allocation.</li> </ul>                                                       |
| Power     | The power consumption in milliwatts (mW) for the PoE port when this command was entered.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Device    | The description of the connected PD device if a description has been added with the <a href="#">power-inline description</a> command. No description is shown for PDs not configured with the <a href="#">power-inline description</a> command.                                                                                                                                                                                                                                                                                            |
| Class     | The class of the connected PD, if power is being supplied to the PD from the PSE. See the <b>Power over Ethernet Introduction</b> chapter for further information about PD classes and the power levels assigned per class.                                                                                                                                                                                                                                                                                                                |
| Max (mW)  | <p>The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port:</p> <ul style="list-style-type: none"> <li>• <b>[U]</b> if the power limit for a port was user configured (with the <a href="#">power-inline max</a> command).</li> <li>• <b>[L]</b> if the power limit for a port was supplied by LLDP.</li> <li>• <b>[C]</b> if the power limit for a port was supplied by the PD class.</li> </ul>                                                                              |

**Related Commands** [show power-inline counters](#)  
[show power-inline interface](#)

# show power-inline counters

**Overview** This command displays Power over Ethernet (PoE) event counters for ports on the Power Sourcing Equipment (PSE). The PoE event counters displayed can also be accessed by objects in the PoE MIB (RFC 3621). See [the MIB Objects Feature Overview and Configuration Guide](#) for information about which PoE MIB objects are supported.

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 power-inline counters [*<port-list>*]

| Parameter                | Description                                                       |
|--------------------------|-------------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | Enter the PoE port(s) to display all PoE event counters for them. |

**Mode** User Exec and Privileged Exec

**Usage** To display all PoE event counters for all PoE ports on the PSE, do not enter the optional interface parameter.

**Examples** To display all PoE event counters for all PoE ports on the PSE, use the command:

```
awplus# show power-inline counters
```

To display the PoE event counters for the port range 1.0.1 to 1.0.3, use the command:

```
awplus# show power-inline counters interface port1.0.1-1.0.3
```

**Output** Figure 14-2: Example output from the **show power-inline counters** command

```
awplus#show power-inline counters interface port1.0.1-port1.0.3
PoE Counters:
Interface MPSAbsent Overload Short Invalid Denied
port1.0.1 0 0 0 0 0
port1.0.2 0 0 0 0 0
port1.0.3 0 0 0 0 0
```

Table 14-2: Parameters in the **show power-inline counters** command output

| Parameter | Description                                                                                                                                                                                                              |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface | The PoE port(s) in the format port x . y . z, where x is the device number, y is the module number within the device, and z is the PoE port number within the module.                                                    |
| MPSAbsent | The number of instances when the PoE MPS (Maintain Power Signature) signal has been lost. The PoE MPS signal is lost when a PD is disconnected from the PSE. Also increments pethPsePortMPSAbsentCounter in the PoE MIB. |
| Over load | The number of instances when a PD exceeds its configured power limit (as configured by the <a href="#">power-inline max</a> command). Also increments pethPsePortOverLoadCounter in the PoE MIB.                         |
| Short     | The number of short circuits that have happened with a PD. Also increments pethPsePortShortCounter in the PoE MIB.                                                                                                       |
| Invalid   | The number of times a PD with an Invalid Signature (where the PD has an open or short circuit, or is a legacy PD) is detected. Also increments pethPseInvalidSignatureCounter in the PoE MIB.                            |
| Denied    | The number of times a PD has been refused power due to power budget limitations for the PSE. Also increments pethPsePortPowerDeniedCounter in the PoE MIB.                                                               |

**Related Commands**

- [clear power-inline counters interface](#)
- [show power-inline](#)
- [show power-inline interface](#)



# show power-inline interface

**Overview** This command displays a summary of Power over Ethernet (PoE) information for specified ports. If no ports are specified then PoE information is displayed for all ports on the Power Sourcing Equipment (PSE).

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 power-inline interface [<port-list>]

| Parameter   | Description                                                                   |
|-------------|-------------------------------------------------------------------------------|
| <port-list> | Enter the PoE port(s) to display PoE specific information in the show output. |

**Mode** User Exec and Privileged Exec

**Usage** To display PoE information for all PoE ports on the PSE, do not specify any ports.

**Example** To display the PoE port specific information for all PoE ports on the switch, use the following command:

```
awplus# show power-inline interface
```

To display the PoE port specific information for the port range 1.0.1 to 1.0.4, use the following command:

```
awplus# show power-inline interface port1.0.1-port1.0.4
```

**Output** Figure 14-3: Example output from the **show power-inline interface** command

|                                                        |          |      |          |       |             |       |         |     |
|--------------------------------------------------------|----------|------|----------|-------|-------------|-------|---------|-----|
| awplus#show power-inline interface port1.0.1-port1.0.4 |          |      |          |       |             |       |         |     |
| Interface                                              | Admin    | Pri  | Oper     | Power | Device      | Class | Max(mW) |     |
| port1.0.1                                              | Disabled | Low  | Disabled | 0     | n/a         | n/a   | n/a     |     |
| port1.0.2                                              | Enabled  | High | Powered  | 3840  | Desk Phone  | 1     | 5000    | [U] |
| port1.0.3                                              | Enabled  | Crit | Powered  | 6720  | AccessPoint | 2     | 7000    | [C] |
| port1.0.4                                              | Disabled | Low  | Disabled | 0     | n/a         | n/a   | n/a     |     |

Table 14-3: Parameters in the **show power-inline interface** command output

| Parameter | Description                                                                                                                                                           |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface | The PoE port(s) in the format port x . y . z, where x is the device number, y is the module number within the device, and z is the PoE port number within the module. |
| Admin     | The administrative state of PoE on a PoE port, either <b>Enabled</b> or <b>Disabled</b> .                                                                             |

Table 14-3: Parameters in the **show power-inline interface** command output

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pri       | <p>The current PoE priorities for PoE ports on the PSE, as configured from a <a href="#">power-inline priority</a> command:</p> <ul style="list-style-type: none"> <li>• <b>Low</b> displays when the low parameter is issued. The lowest priority for a PoE enabled port (default).</li> <li>• <b>High</b> displays when the high parameter is issued. The second highest priority for a PoE enabled port.</li> <li>• <b>Crit</b> displays when the critical parameter is issued. The highest priority for a PoE enabled port.</li> </ul>                         |
| Oper      | <p>The current PSE PoE port state when this command was issued:</p> <ul style="list-style-type: none"> <li>• <b>Powered</b> displays when there is a PD connected and power is being supplied from the PSE.</li> <li>• <b>Denied</b> displays when supplying power would make the PSE go over the power budget.</li> <li>• <b>Disabled</b> displays when the PoE port is administratively disabled.</li> <li>• <b>Off</b> displays when PoE has been disabled for the port.</li> <li>• <b>Fault</b> displays when a PSE goes over its power allocation.</li> </ul> |
| Power     | The power consumption in milliwatts (mW) for the PoE port when this command was entered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Device    | The description of the connected PD device if a description has been added with the <a href="#">power-inline description</a> command. No description is shown for PDs not configured with the <a href="#">power-inline description</a> command.                                                                                                                                                                                                                                                                                                                    |
| Class     | <p>The class of the connected PD, if power is being supplied to the PD from the PSE.</p> <p>See the <a href="#">PoE Feature Overview and Configuration Guide</a> for further information about power classes.</p>                                                                                                                                                                                                                                                                                                                                                  |
| Max (mW)  | <p>The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port:</p> <ul style="list-style-type: none"> <li>• <b>[U]</b> if the power limit for a port was user configured (with the <b>power-inline max</b> command).</li> <li>• <b>[L]</b> if the power limit for a port was supplied by LLDP.</li> <li>• <b>[C]</b> if the power limit for a port was supplied by the PD class.</li> </ul>                                                                                                               |

**Related Commands** [show power-inline](#)  
[show power-inline interface detail](#)

# show power-inline interface detail

**Overview** This command displays detailed information for specified Power over Ethernet (PoE) port(s) on the Power Sourcing Equipment (PSE).

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 power-inline interface [*<port-list>*] detail

| Parameter                | Description                                                         |
|--------------------------|---------------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | Enter the PoE port(s) to display the PoE port specific information. |

**Mode** User Exec and Privileged Exec

**Usage** To show detailed PoE information for all ports on the PSE, do not specify any ports.

The power allocated to each port is listed in the Power allocated row, and is limited by the maximum power per Powered Device (PD) class, or a user configured power limit.

**Example** To display detailed PoE port specific information for the port range 1.0.1 to 1.0.2, use the following command:

```
awplus# show power-inline interface port1.0.1-port1.0.2 detail
```

**Output** Figure 14-4: Example output from the **show power-inline interface detail** command

```
awplus#show power-inline interface port1.0.1-1.0.2 detail
Interface port1.0.1
 Powered device type: Desk Phone #1
 PoE admin enabled
 Priority Low
 Detection status: Powered
 Current power consumption: 4800 mW
 Powered device class: 1
 Power allocated: 5000 mW (from configuration)
 Detection of legacy devices is disabled
 Powered pairs: Data
Interface port1.0.2
 Powered device type: Access Point #3
 PoE admin enabled
 Priority High
 Detection status: Powered
 Current power consumption: 6720 mW
 Powered device class: 2
 Power allocated: 7000 mW (from powered device class)
 Detection of legacy devices is enabled
 Powered pairs: Data
```

Table 14-4: Parameters in **show power-inline interface detail** command output

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Interface            | The PoE port(s) in the format port x . y . z, where x is the device number, y is the module number within the device, and z is the PoE port number within the module.                                                                                                                                                                                                                                                                                                                                                                                       |
| Powered device type: | The name of the PD, if connected and if power is being supplied to the PD from the PSE, configured with the <a href="#">power-inline description</a> command. <b>n/a</b> displays if a description has not been configured for the PD.                                                                                                                                                                                                                                                                                                                      |
| PoE admin            | The administrative state of PoE on a PoE capable port, either <b>Enabled</b> or <b>Disabled</b> as configured from the <a href="#">power-inline enable</a> command or the <b>no power-inline enable</b> command respectively.                                                                                                                                                                                                                                                                                                                               |
| Priority             | The PoE priority of a port, which is either <b>Low</b> , or <b>High</b> , or <b>Critical</b> , as configured by the <a href="#">power-inline priority</a> command.                                                                                                                                                                                                                                                                                                                                                                                          |
| Detection status:    | The current PSE PoE port state when this command was issued: <ul style="list-style-type: none"> <li>• <b>Powered</b> displays when there is a PD connected and power is being supplied from the PSE.</li> <li>• <b>Denied</b> displays when supplying power would make the PSE go over the power budget.</li> <li>• <b>Disabled</b> displays when the PoE port is administratively disabled.</li> <li>• <b>Off</b> displays when PoE has been disabled for the port.</li> <li>• <b>Fault</b> displays when a PSE goes over its power allocation.</li> </ul> |

Table 14-4: Parameters in **show power-inline interface detail** command output

| Parameter                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Current power consumption:     | The power consumption for the PoE port when this command was entered. Note that the power consumption may have changed since the command was entered and the power is displayed.                                                                                                                                                                                                                                                              |
| Powered device class:          | The class of the connected PD if connected, and if power is being supplied to the PD from the PSE.<br>See the <a href="#">PoE Feature Overview and Configuration Guide</a> for further information about power classes.                                                                                                                                                                                                                       |
| Power allocated:               | The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port: <ul style="list-style-type: none"> <li>• <b>[U]</b> if the power limit for a port was user configured (with the <b>power-inline max</b> command).</li> <li>• <b>[L]</b> if the power limit for a port was supplied by LLDP.</li> <li>• <b>[C]</b> if the power limit for a port was supplied by the PD class.</li> </ul> |
| Detection of legacy devices is | [Enabled Disabled]<br>The status of legacy PoE detection on the PoE port, as configured for the PoE port with the <a href="#">power-inline allow-legacy</a> command.                                                                                                                                                                                                                                                                          |
| Powered pairs:                 | [Data   Spare]<br>The IEEE 802.3af and IEEE 802.3at standards allow for either <b>data</b> or <b>spare</b> twisted pairs to be used to transfer power to a PD. The powered pairs status for each port. AlliedWare Plus™ PoE switches implement IEEE 802.3af and IEEE 802.3at Endpoint PSE Alternative A ( <b>Data</b> ).                                                                                                                      |

**Related Commands** [show power-inline](#)  
[show power-inline interface](#)

# 15

# GVRP Commands

## Introduction

**Overview** With GVRP enabled the switch can exchange VLAN configuration information with other GVRP enabled switches. VLANs can be dynamically created and managed through trunk ports.

GVRP is supported in Software Version 5.4.3A-1.x and later.

- There is limit of 400 VLANs supported by the AlliedWare Plus GVRP implementation. VLANs may be numbered 1-4094, but a limit of 400 of these VLANs are supported.
- MSTP is not supported by the AlliedWare Plus GVRP implementation. GVRP and MSTP are mutually exclusive. STP and RSTP are supported by GVRP.

This chapter provides an alphabetical reference for commands used to configure GVRP. For information about GVRP, including configuration, see the [GVRP Feature Overview and Configuration Guide](#).

- Command List**
- [“clear gvrp statistics”](#) on page 527
  - [“debug gvrp”](#) on page 528
  - [“gvrp \(interface\)”](#) on page 530
  - [“gvrp dynamic-vlan-creation”](#) on page 531
  - [“gvrp enable \(global\)”](#) on page 532
  - [“gvrp registration”](#) on page 533
  - [“gvrp timer”](#) on page 534
  - [“show debugging gvrp”](#) on page 535
  - [“show gvrp configuration”](#) on page 536
  - [“show gvrp machine”](#) on page 537
  - [“show gvrp statistics”](#) on page 538
  - [“show gvrp timer”](#) on page 539

# clear gvrp statistics

**Overview** Use this command to clear the GVRP statistics for all switchports, or for a specific switchport.

**Syntax** `clear gvrp statistics {all|<interface>}`

| Parameter   | Description                                       |
|-------------|---------------------------------------------------|
| all         | Specify all switchports to clear GVRP statistics. |
| <interface> | Specify the switchport to clear GVRP statistics.  |

**Mode** Privileged Exec

**Usage** Use this command together with the [show gvrp statistics](#) command to troubleshoot GVRP.

**Examples** To clear all GVRP statistics for all switchport on the switch, enter the command:  
`awplus# clear gvrp statistics all`

**Related  
Commands** [show gvrp statistics](#)

# debug gvrp

**Overview** Use this command to debug GVRP packets and commands, sending output to the console.

Use the **no** variant of this command to turn off debugging for GVRP packets and commands.

**Syntax** debug gvrp {all|cli|event|packet}  
no debug gvrp {all|cli|event|packet}

| Parameter | Description                         |
|-----------|-------------------------------------|
| all       | Specifies debugging for all levels. |
| cli       | Specifies debugging for commands.   |
| event     | Specified debugging for events.     |
| packet    | Specifies debugging for packets.    |

**Mode** Privileged Exec and Global Configuration

**Examples** To send debug output to the console for GVRP packets and GVRP commands, and to enable the display of debug output on the console first, enter the commands:

```
awplus# terminal monitor
awplus# configure terminal
awplus(config)# debug gvrp all
```

To send debug output for GVRP packets to the console, enter the commands:

```
awplus# terminal monitor
awplus# configure terminal
awplus(config)# debug gvrp packets
```

To send debug output for GVRP commands to the console, enter the commands:

```
awplus# terminal monitor
awplus# configure terminal
awplus(config)# debug gvrp cli
```

To stop sending debug output for GVRP packets and GVRP commands to the console, and to stop the display of any debug output on the console, enter the commands:

```
awplus# terminal no monitor
awplus# configure terminal
awplus(config)# no debug gvrp all
```



**Related  
Commands**    [show debugging gvrp](#)  
[terminal monitor](#)

## gvrp (interface)

**Overview** Use this command to enable GVRP for switchport interfaces.  
Use the **no** variant of this command to disable GVRP for switchport interfaces.

**Syntax** gvrp  
no gvrp

**Mode** Interface Configuration (for switchport interfaces).

**Default** Disabled by default.

**Usage** Use this command to enable GVRP on switchport interfaces. Note this command does not enable GVRP for the switch. To enable GVRP on switchports use this command in Interface Configuration mode. You must issue a [gvrp enable \(global\)](#) command before issuing a [gvrp \(interface\)](#) command.

You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.

**NOTE:** MSTP is not supported by the current AlliedWare Plus GVRP implementation. GVRP and MSTP are mutually exclusive. STP and RSTP are supported by GVRP.

Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. GVRP and private VLAN trunk ports are mutually exclusive.

**Validation Commands** [show gvrp configuration](#)

**Related Commands** [gvrp dynamic-vlan-creation](#)  
[gvrp enable \(global\)](#)

# gvrp dynamic-vlan-creation

**Overview** Use this command to enable dynamic VLAN creation globally for the switch.  
Use the **no** variant of this command to disable dynamic VLAN creation globally for the switch.

**Syntax** gvrp dynamic-vlan-creation  
no gvrp dynamic-vlan-creation

**Mode** Global Configuration

**Default** Disabled by default.

**Usage** You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.  
You must also enable GVRP globally in Global Configuration mode before enabling GVRP on an interface in Interface Configuration mode. Both of these tasks must occur to create VLANs.

**NOTE:** *There is limit of 400 VLANs supported by the AlliedWare Plus GVRP implementation. VLANs may be numbered 1-4094, but a limit of 400 of these VLANs are supported.*

**Examples** Enter the following commands for switches with hostnames switch1 and switch2 respectively, so switch1 propagates VLANs to switch2 and switch2 propagates VLANs to switch1:

Switch1:

```
switch1# configure terminal
switch1(config)# gvrp enable
switch1(config)# gvrp dynamic-vlan-creation
```

Switch2:

```
switch2# configure terminal
switch2(config)# gvrp enable
switch2(config)# gvrp dynamic-vlan-creation
```

To disable GVRP dynamic VLAN creation on the switch, enter the commands:

```
awplus# configure terminal
awplus(config)# no gvrp dynamic-vlan-creation
```

**Validation Commands** [show gvrp configuration](#)

**Related Commands** [gvrp enable \(global\)](#)

# gvrp enable (global)

**Overview** Use this command to enable GVRP globally for the switch.

GVRP is supported in Software Version 5.4.3A-1.x and later.

Use the **no** variant of this command to disable GVRP globally for the switch.

**Syntax** gvrp enable  
no gvrp enable

**Mode** Global Configuration

**Default** Disabled by default.

**Usage** Use this command to enable GVRP on the switch. Note that this command does not enable GVRP on switchports. To enable GVRP on switchports use the [gvrp \(interface\)](#) command in Interface Configuration mode. You must issue a [gvrp enable \(global\)](#) command before issuing a [gvrp \(interface\)](#) command.

You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.

**NOTE:** MSTP is not supported by the current AlliedWare Plus GVRP implementation. GVRP and MSTP are mutually exclusive. STP and RSTP are supported by GVRP.

Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. GVRP and private VLAN trunk ports are mutually exclusive.

**Examples** To enable GVRP for the switch, before enabling GVRP on switchports, enter the commands:

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

To disable GVRP on the switch, which will also disable GVRP enabled on switchports, enter the commands:

```
awplus# configure terminal
awplus(config)# no gvrp enable
```

**Validation Commands** [show gvrp configuration](#)

**Related Commands** [gvrp \(interface\)](#)  
[gvrp dynamic-vlan-creation](#)

# gvrp registration

**Overview** Use this command to set GVRP registration to normal, fixed, and forbidden registration modes.

Use the **no** variant of this command to disable GVRP registration.

**Syntax** gvrp registration {normal|fixed|forbidden}  
no gvrp registration {normal|fixed|forbidden}

| Parameter | Description                                                    |
|-----------|----------------------------------------------------------------|
| normal    | Specify dynamic GVRP registration and deregistration of VLANs. |
| fixed     | Specify fixed GVRP registration and deregistration of VLANs.   |
| forbidden | Specify no GVRP registration of VLANs. VLANs are deregistered. |

**Mode** Interface Configuration

**Default** Normal registration is the default.

**Usage** Configuring a trunk port in normal registration mode allows dynamic creation of VLANs. Normal mode is the default mode. Validate using the [show gvrp configuration](#) command.

Configuring a trunk port in fixed registration mode allows manual creation of VLANs.

Configuring a trunk port in forbidden registration mode prevents VLAN creation on the port.

**Validation Commands** [show gvrp configuration](#)

## gvrp timer

**Overview** Use this command to set GVRP timers in Interface Configuration mode for a given interface.

Use the **no** variant of this command to reset the GVRP timers to the defaults specified in the table below.

**Syntax** `gvrp timer {join <timer-value>|leave <timer-value>|leaveall <timer-value>}`  
`no gvrp timer {join|leave|leaveall}`

| Parameter     | Description                                                                                                                 |
|---------------|-----------------------------------------------------------------------------------------------------------------------------|
| join          | Specifies the timer for joining the group (default is 20 centiseconds / hundredths of a second, or 200 milliseconds).       |
| leave         | Specifies the timer for leaving a group (default is 60 centiseconds / hundredths of a second, or 600 milliseconds).         |
| leaveall      | Specifies the timer for leaving all groups (default is 1000 centiseconds / hundredths of a second, or 10,000 milliseconds). |
| <timer-value> | <1-65535> The timer value in hundredths of a second (centiseconds).                                                         |

**Mode** Interface Configuration

**Defaults** The default join time value is 20 centiseconds (200 milliseconds), the default leave timer value is 60 centiseconds (600 milliseconds), and the default leaveall timer value is 1000 centiseconds (10,000 milliseconds).

**Usage** When configuring the leave timer, set it to more than or equal to three times the join timer value. The settings for the leave and join timers must be the same for all GVRP enabled switches. See also the section “Setting the GVRP Timers” in the [GVRP Feature Overview and Configuration Guide](#).

Use the [show gvrp timer](#) command to confirm GVRP timers set with this command.

**Related Commands** [show gvrp timer](#)

# show debugging gvrp

**Overview** Use this command to display the GVRP debugging option set.

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 debugging gvrp

**Mode** User Exec and Privileged Exec

**Example** Enter the following commands to display GVRP debugging output on the console:

```
awplus# configure terminal
awplus(config)# debug gvrp all
awplus(config)# exit
awplus# show debugging gvrp
```

**Output** See sample output from the **show debugging gvrp** command after entering **debug gvrp all**:

```
GVRP debugging status:
GVRP Event debugging is on
GVRP CLI debugging is on
GVRP Timer debugging is on
GVRP Packet debugging is on
```

**Related  
Commands** [debug gvrp](#)

# show gvrp configuration

- Overview** Use this command to display GVRP configuration data for a switch.
- 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 gvrp configuration
- Mode** User Exec and Privileged Exec
- Example** To show GVRP configuration for the switch, enter the command:
- ```
awplus# show gvrp configuration
```
- Output** The following is an output of this command displaying the GVRP configuration for a switch:

show gvrp machine

- Overview** Use this command to display the state machine for GVRP.
- 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 gvrp machine
- Mode** User Exec and Privileged Exec
- Example** To show the GVRP state machine for the switch, enter the command:
- ```
awplus# show gvrp machine
```
- Output** See the following output of this command displaying the GVRP state machine.

# show gvrp statistics

**Overview** Use this command to display a statistical summary of GVRP information for the switch.

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 gvrp statistics [<interface>]

| Parameter   | Description                           |
|-------------|---------------------------------------|
| <interface> | The name of the switchport interface. |

**Mode** User Exec and Privileged Exec

**Usage** Use this command together with the [clear gvrp statistics](#) command to troubleshoot GVRP.

**Examples** To show the GVRP statistics for all switchport interfaces, enter the command:  
awplus# show gvrp statistics

**Related Commands** [clear gvrp statistics](#)

# show gvrp timer

**Overview** Use this command to display data for the GVRP timers set with the [gvrp timer](#) command.

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 gvrp timer <interface>

| Parameter   | Description                           |
|-------------|---------------------------------------|
| <interface> | The name of the switchport interface. |

**Mode** User Exec and Privileged Exec

**Examples** To show the GVRP timers for all switchport interfaces, enter the command:  
awplus# show gvrp timer

**Related Commands** [gvrp timer](#)

# 16

# IP Addressing and Protocol Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure the following protocols:

- Address Resolution Protocol (ARP)
- Domain Name Service (DNS)

For more information, see the [IP Feature Overview and Configuration Guide](#).

- Command List**
- ["arp-aging-timeout"](#) on page 542
  - ["arp-mac-disparity"](#) on page 543
  - ["arp \(IP address MAC\)"](#) on page 544
  - ["arp log"](#) on page 545
  - ["clear arp-cache"](#) on page 549
  - ["debug ip packet interface"](#) on page 550
  - ["ip address"](#) on page 552
  - ["ip domain-list"](#) on page 554
  - ["ip domain-lookup"](#) on page 555
  - ["ip domain-name"](#) on page 556
  - ["ip gratuitous-arp-link"](#) on page 557
  - ["ip name-server"](#) on page 559
  - ["ping"](#) on page 560
  - ["show arp"](#) on page 561
  - ["show debugging ip packet"](#) on page 563
  - ["show hosts"](#) on page 565
  - ["show ip domain-list"](#) on page 566

- [“show ip domain-name”](#) on page 567
- [“show ip interface”](#) on page 568
- [“show ip name-server”](#) on page 569
- [“show ip sockets”](#) on page 570
- [“show ip traffic”](#) on page 573
- [“tcpdump”](#) on page 579
- [“traceroute”](#) on page 580
- [“undebbug ip packet interface”](#) on page 581

# arp-aging-timeout

**Overview** This command sets a timeout period on dynamic ARP entries associated with a specific interface. If your device stops receiving traffic for the host specified in a dynamic ARP entry, it deletes the ARP entry from the ARP cache after this timeout is reached.

Your device times out dynamic ARP entries to ensure that the cache does not fill with entries for hosts that are no longer active. Static ARP entries are not aged or automatically deleted.

By default the time limit for dynamic ARP entries is 300 seconds on all interfaces. The **no** variant of this command sets the time limit to the default of 300 seconds.

**Syntax** `arp-aging-timeout <0-432000>`  
`no arp-aging timeout`

| Parameter                     | Description                    |
|-------------------------------|--------------------------------|
| <code>&lt;0-432000&gt;</code> | The timeout period in seconds. |

**Default** 300 seconds (5 minutes)

**Mode** Interface Configuration for a VLAN interface.

**Example** To set the ARP entries on interface `vlan30` to time out after two minutes, use the commands:

```
awplus(config)# interface vlan30
awplus(config-if)# arp-aging-timeout 120
```

**Related  
Commands** [clear arp-cache](#)  
[show arp](#)

# arp-mac-disparity

**Overview** Use this command in Interface Configuration mode for a VLAN interface to enable the reception of ARP packets that contain a multicast MAC address in the sender field.

By default, ARP packets that contain a multicast MAC address in the sender field are dropped. The **no** variant of this command reverts to the default behavior.

**Syntax** `arp-mac-disparity`  
`no arp-mac-disparity`

**Default** ARP disparity is disabled. ARP packets with a multicast MAC address in the sender field are dropped.

**Mode** Interface Configuration for a VLAN interface.

**Usage** Normally, it is invalid for an ARP request to resolve a multicast MAC address. By default, ARP replies with a multicast MAC addresses are not learned. This command allows control over the learning of dynamic ARPs that resolve to a multicast MAC address.

ARP-MAC disparity may need to be enabled to support multicast network load balancing. The `arp-mac-disparity` command allows ARP replies quoting multicast MAC addresses to be accepted and learned. No `arp-mac-disparity` command reverts to default behavior.

If the ARP-MAC disparity feature is enabled, then the device sends traffic to a single port as specified by the ARP entry.

**Examples** To enable ARP MAC disparity on interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-mac-disparity
```

To disable ARP MAC disparity on interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no arp-mac-disparity
```

**Related  
Commands** `clear arp-cache`  
`show arp`

## arp (IP address MAC)

**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> [<port-number>] [alias]`  
`no arp <ip-addr>`

| Parameter                        | Description                                                                                                                               |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-addr&gt;</code>     | IPv4 address of the device you are adding as a static ARP entry.                                                                          |
| <code>&lt;mac-address&gt;</code> | MAC address of the device you are adding as a static ARP entry, in hexadecimal notation with the format HHHH.HHHH.HHHH.                   |
| <code>&lt;port-number&gt;</code> | The port number associated with the IP address. Specify this when the IP address is part of a VLAN.                                       |
| <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 0010.2533.4655 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 0010.2355.4566 alias
```

**Related Commands** [clear arp-cache](#)  
[show arp](#)



# arp log

**Overview** This command enables the logging of dynamic and static ARP entries in the ARP cache. The ARP cache contains mappings of device ports, VLAN IDs, and IP addresses to physical MAC addresses for hosts.

This command can display the MAC addresses in the ARP log either using the default hexadecimal 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 dynamic and static ARP entries in the ARP cache.

**Syntax** `arp log [mac-address-format ieee]`  
`no arp log [mac-address-format ieee]`

| Parameter               | Description                                                                                                                                                                                    |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| mac-address-format ieee | Display the MAC address in hexadecimal notation with the standard IEEE format (HH-HH-HH-HH-HH-HH), instead of displaying the MAC address with the default hexadecimal format (HHHH.HHHH.HHHH). |

**Default** The ARP logging feature is disabled by default.

**Mode** Global Configuration

**Usage** You have the option to change how the MAC address is displayed in the ARP log message, to use the default hexadecimal notation (HHHH.HHHH.HHHH), or the IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH) when you apply the **mac-address-format ieee** parameter.

Enter the **arp log** command without the optional **mac-address-format ieee** parameter specified for MAC addresses in the ARP log output to use the default hexadecimal notation (HHHH.HHHH.HHHH).

Enter the **arp log mac-address-format ieee** command for MAC addresses in the ARP log output to use the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH).

Use the **no** variant of this command (**no arp log**) without the optional **mac-address-format ieee** parameter specified to disable ARP logging on the device

Use the **no** variant of this command with the optional **mac-address-format ieee** parameter specified (**no arp log mac-address-format ieee**) to disable IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) and revert to the default hexadecimal notation (HHHH.HHHH.HHHH) for MAC addresses in the ARP log output.

To display ARP log messages use the **show log | include ARP\_LOG** command.

**Examples** To enable ARP logging and use the default hexadecimal notation (HHHH.HHHH.HHHH), use the following commands:

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

To disable ARP logging on the device of MAC addresses displayed using the default hexadecimal notation (HHHH.HHHH.HHHH), use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log
```

To enable ARP logging and to 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 disable ARP logging on the device of MAC addresses displayed using the standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH), and revert to the use of the default hexadecimal notation (HHHH.HHHH.HHHH) instead, use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log mac-address-format ieee
```

To display ARP log messages, use following command:

```
awplus# show log | include ARP_LOG
```

**Output** Below is example output from the **show log | include ARP\_LOG** command after enabling ARP logging displaying default hexadecimal notation MAC addresses (HHHH.HHHH.HHHH) using the **arp log** command.

```
awplus#configure terminal
awplus(config)#arp log
awplus(config)#exit
awplus#show log | include ARP_LOG
2010 Apr 6 06:21:01 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add
0013.4078.3b98 (192.168.2.4)
2010 Apr 6 06:22:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del
0013.4078.3b98 (192.168.2.4)
2010 Apr 6 06:23:26 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add
0030.940e.136b (192.168.2.20)
2010 Apr 6 06:23:30 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Below is example output from the **show log | include ARP\_LOG** command after enabling ARP logging displaying IEEE standard format hexadecimal notation MAC

addresses (HH-HH-HH-HH-HH-HH) using the **arp log mac-address format ieee** command.

Table 16-1: Example output from the **show log | include ARP\_LOG** command

```
awplus#configure terminal
awplus(config)#arp log mac-address-format ieee
awplus(config)#exit
awplus#show log | include ARP_LOG
2010 Apr 6 06:25:28 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add 00-17-9a-b6-03-69 (192.168.2.12)
2010 Apr 6 06:25:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add 00-03-37-6b-a6-a5 (192.168.2.10)
2010 Apr 6 06:26:53 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-30-94-0e-13-6b (192.168.2.20)
2010 Apr 6 06:27:31 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-17-9a-b6-03-69 (192.168.2.12)
2010 Apr 6 06:28:09 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-03-37-6b-a6-a5 (192.168.2.10)
2010 Apr 6 06:28:14 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Below are the parameters in output of the **show log | include ARP\_LOG** command with an ARP log message format of <ARP\_LOG> <port number> <VLAN ID> <Operation> <MAC> <IP> after <date> <time> <severity> <hostname> <program-name> information.

Table 16-2: Parameters in output of the **show log | include ARP\_LOG** command

| Parameter     | Description                                                                                                                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ARP_LOG>     | Indicates ARP log entry information follows <date> <time> <severity> <hostname> <program name> log information.                                                                                                                                                                  |
| <port number> | Indicates device port number for the ARP log entry.                                                                                                                                                                                                                              |
| <VLAN ID>     | Indicates the VLAN ID for the ARP log entry.                                                                                                                                                                                                                                     |
| <Operation>   | Indicates 'add' if the ARP log entry displays an ARP addition. Indicates 'de l ' 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 <b>arp log</b> or the <b>arp log mac-address-format ieee</b> command. |
| <IP>          | Indicates the IP address for the ARP log entry.                                                                                                                                                                                                                                  |

**Validation Commands** [show running-config](#)

**Related Commands** [show log](#)

# 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>]`

**Mode** Privileged Exec

**Usage** 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 \(IP address MAC\)](#) 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-mac-disparity](#)
- [arp \(IP address MAC\)](#)
- [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 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>  | Specify a single Layer 3 interface name (not a range of interfaces)<br>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.<br>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 <b>verbose</b> to output more of the IP packet.<br>If this keyword is specified then more of the packet is shown in the output.                                                                                |
| hex          | Specify <b>hex</b> to output the IP packet in hexadecimal.<br>If this keyword is specified, then the output for the packet is shown in hex.                                                                            |
| arp          | Specify <b>arp</b> to output ARP protocol packets.<br>If this keyword is specified, then ARP packets are shown in the output.                                                                                          |
| udp          | Specify <b>udp</b> to output UDP protocol packets.<br>If this keyword is specified then UDP packets are shown in the output.                                                                                           |
| tcp          | Specify <b>tcp</b> to output TCP protocol packets.<br>If this keyword is specified, then TCP packets are shown in the output.                                                                                          |
| icmp         | Specify <b>icmp</b> to output ICMP protocol packets.<br>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 v lan1, use the command:

```
awplus# debug ip packet interface vlan1 arp
```

To turn on all packet debugging on all interfaces on the device, use the command:

```
awplus# debug ip packet interface all
```

To turn on TCP packet debugging on v lan1 and IP address 192 . 168 . 2 . 4, use the command:

```
awplus# debug ip packet interface vlan1 address 192.168.2.4 tcp
```

To turn off IP packet interface debugging on all interfaces, use the command:

```
awplus# no debug ip packet interface
```

To turn off IP packet interface debugging on interface v lan2, use the command:

```
awplus# no debug ip packet interface vlan2
```

**Related  
Commands**

[no debug all](#)

[tcpdump](#)

[terminal monitor](#)

[undebug ip packet interface](#)

# ip address

**Overview** This command sets a static IP address on an interface. To set the primary IP address on the interface, specify only **ip address**<ip-address/m>. 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 not **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.

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]  
no ip address

| 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 a VLAN interface or a local loopback interface.

**Examples** To add the primary IP address 10 . 10 . 10 . 50/24 to the interface v l a n 3, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan3
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 vlan3
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
```

**Related  
Commands**

- interface (to configure)
- show ip interface
- show running-config interface



# ip domain-list

**Overview** This command adds a domain to the DNS list. Domain 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>&lt;domain-name&gt;</code> | Domain string, for example "company.com". |

**Mode** Global Configuration

**Usage** 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.

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`  
`no ip domain-lookup`

**Mode** Global Configuration

**Usage** The client is enabled by default. However, it does not attempt DNS inquiries unless there is a DNS server configured.

For more information about DNS clients, see the [IP Feature Overview and Configuration Guide](#).

**Examples** To enable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup
```

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 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>`

| Parameter                        | Description                               |
|----------------------------------|-------------------------------------------|
| <code>&lt;domain-name&gt;</code> | Domain string, for example "company.com". |

**Mode** Global Configuration

**Usage** 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 gratuitous-arp-link

**Overview** This command sets the Gratuitous ARP time limit for all switchports. The time limit restricts the sending of Gratuitous ARP packets to one Gratuitous ARP packet within the time in seconds.

**NOTE:** This command specifies time between sequences of Gratuitous ARP packets, and time between individual Gratuitous ARP packets occurring in a sequence, to allow legacy support for older devices and interoperability between other devices that are not ready to receive and forward data until several seconds after linkup.

Additionally, jitter has been applied to the delay following linkup, so Gratuitous ARP packets applicable to a given port are spread over a period of 1 second so are not all sent at once. Remaining Gratuitous ARP packets in the sequence occur after a fixed delay from the first one.

**Syntax** ip gratuitous-arp-link <0-300>  
no ip gratuitous-arp-link

| Parameter | Description                                                                                                                                                                                                                     |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <0-300>   | Specify the minimum time between sequences of Gratuitous ARPs and the fixed time between Gratuitous ARPs occurring in a sequence, in seconds.<br>0 disables the sending of Gratuitous ARP packets.<br>The default is 8 seconds. |

**Default** The default Gratuitous ARP time limit for all switchports is 8 seconds.

**Mode** Global Configuration

**Usage** Every switchport will send a sequence of 3 Gratuitous ARP packets to each VLAN that the switchport is a member of, whenever the switchport moves to the forwarding state. The first Gratuitous ARP packet is sent 1 second after the switchport becomes a forwarding switchport. The second and third Gratuitous ARP packets are each sent after the time period specified by the Gratuitous ARP time limit.

Additionally, the Gratuitous ARP time limit specifies the minimum time between the end of one Gratuitous ARP sequence and the start of another Gratuitous ARP sequence. When a link is flapping, the switchport's state is set to forwarding several times. The Gratuitous ARP time limit is imposed to prevent Gratuitous ARP packets from being sent undesirably often.

**Examples** To disable the sending of Gratuitous ARP packets, use the commands :

```
awplus# configure terminal
awplus(config)# ip gratuitous-arp-link 0
```

To restrict the sending of Gratuitous ARP packets to one every 20 seconds, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# ip gratuitous-arp-link 20
```

**Validation**    `show running-config`  
**Commands**

# ip name-server

**Overview** This command adds 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>`  
`no ip name-server <ip-addr>`

**Mode** Global Configuration

**Usage** When your device is using its DHCP client for an interface, it can receive Option 6 messages from the DHCP server. This option appends the name server list with more DNS servers.

For more information about DHCP and DNS, see the [IP 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
```

**Related Commands** [ip domain-list](#)  
[ip domain-lookup](#)  
[ip domain-name](#)  
[show ip name-server](#)

# 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
```

# 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show arp [security [interface [<interface-list>]]  
show arp [statistics [detail][interface [<interface-list>]]

**Mode** User Exec and Privileged Exec

**Usage** 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 16-1: Example output from the **show arp** command

| awplus#show<br>arp |                |           |           |         |
|--------------------|----------------|-----------|-----------|---------|
| IP Address         | MAC Address    | Interface | Port      | Type    |
| 192.168.10.2       | 0015.77ad.fad8 | vlan1     | port1.0.1 | dynamic |
| 192.168.20.2       | 0015.77ad.fa48 | vlan2     | port1.0.2 | dynamic |
| 192.168.1.100      | 00d0.6b04.2a42 | vlan2     | port1.0.6 | static  |

Table 16-3: Parameters in the output of the **show arp** command

| Parameter   | Meaning                                                                                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IP Address  | IP address of the network device this entry maps to.                                                                                                                                                   |
| MAC 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 <a href="#">arp (IP address MAC)</a> command. Dynamic entries are learned from ARP request/reply message exchanges. |



**Related  
Commands**    arp (IP address MAC)  
                  clear arp-cache

# show debugging ip packet

**Overview** Use this command to show the IP interface debugging status. IP interface debugging is set using the **debug ip packet interface** command.

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 debugging ip packet

**Mode** User Exec and Privileged Exec

**Example** To display the IP interface debugging status when the terminal monitor off, use the command:

```
awplus# terminal no monitor
awplus# show debug ip packet
```

**Output** Figure 16-2: Example output from the **show debugging ip packet** command with **terminal monitor** off

```
awplus#terminal no monitor
awplus#show debug ip packet
IP debugging status:
interface all tcp (stopped)
interface vlan1 arp verbose (stopped)
```

**Example** To display the IP interface debugging status when the terminal monitor is on, use the command:

```
awplus# terminal monitor
awplus# show debug ip packet
```

**Output** Figure 16-3: Example output from the **show debugging ip packet** command with **terminal monitor** on

```
awplus#terminal monitor
awplus#show debug ip packet
IP debugging status:
interface all tcp (running)
interface vlan1 arp verbose (running)
```

**Related  
Commands**    [debug ip packet interface](#)  
[terminal monitor](#)

# 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 “Controlling “show” Command Output” in 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 16-4: Example output from the **show hosts** command

```
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
```

**Related  
Commands**

- [ip domain-list](#)
- [ip domain-lookup](#)
- [ip domain-name](#)
- [ip name-server](#)

# 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 “Controlling “show” Command Output” in 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 16-5: 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 “Controlling “show” Command Output” in 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 16-6: 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 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 “Controlling “show” Command Output” in 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: <ul style="list-style-type: none"><li>• an interface, e.g. v lan2</li><li>• a continuous range of interfaces separated by a hyphen, e.g. v lan2 - 8 or v lan2 - v lan5</li><li>• a comma-separated list of interfaces or interface ranges, e.g. v lan2, v lan5, v lan8 - 10</li></ul> The specified interfaces must exist. |

**Mode** User Exec and Privileged Exec

**Examples** To show brief information for the assigned IP address for interface port1.0.2 use the command:

```
awplus# show ip interface port1.0.2 brief
```

To show the IP addresses assigned to vlan2 and vlan3, use the command:

```
awplus# show ip interface vlan2-3 brief
```

**Output** Figure 16-7: Example output from the **show ip interface brief** command

| Interface | IP-Address  | Status   | Protocol |
|-----------|-------------|----------|----------|
| port1.0.2 | unassigned  | admin up | down     |
| vlan1     | 192.168.1.1 | admin up | running  |
| vlan2     | 192.168.2.1 | admin up | running  |
| vlan3     | 192.168.3.1 | admin up | running  |
| vlan8     | unassigned  | admin up | down     |

# 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.

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 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 16-8: Example output from the **show ip name-server** command

```
awplus# show ip name-server
10.10.0.123
10.10.0.124
2001:0db8:010d::1
```

**Related Commands** [ip domain-lookup](#)  
[ip name-server](#)



# 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, UDP listen sockets, displaying 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 ICMP6, which are configured to receive IP packets with the associated protocol number.

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 ip sockets

**Mode** Privileged Exec

**Usage** 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 the **show ip sockets** command

| 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 16-4: Parameters in the output of the **show ip sockets** command

| Parameter                                              | Description                                                                                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Not showing<br><number><br>local<br>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<br><number><br>local<br>listening<br>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.                                                                                    |
| Typ                                                    | This column displays the type of the socket. Possible values for this column are:<br>tcp : IP Protocol 6<br>udp : IP Protocol 17<br>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. |

Table 16-4: Parameters in the output of the **show ip sockets** command (cont.)

| Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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: <a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a> |
| 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:<br>LISTEN<br>SYN-SENT<br>SYN-RECEIVED<br>ESTABLISHED<br>FIN-WAIT-1<br>FIN-WAIT-2<br>CLOSE-WAIT<br>CLOSING<br>LAST-ACK<br>TIME-WAIT<br>CLOSED<br>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 “Controlling “show” Command Output” in 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

```

IP:
 261998 packets received
 261998 delivered
 261998 sent
 69721 multicast packets received
 69721 multicast packets sent
 23202841 bytes received
 23202841 bytes sent
 7669296 multicast bytes received
 7669296 multicast bytes sent
IPv6:
 28 packets discarded on transmit due to no route
ICMP6:
UDP6:
UDPLite6:
TCP:
 0 remote connections established
 40 local connections established
 7 remote listening ports
 7 local listening ports
 261 active connection openings
 247 passive connection openings
 14 connection attempts failed
 122535 segments received
 122535 segments transmitted
 14 resets transmitted
 227 TCP sockets finished time wait in fast timer
 155 delayed acks sent
 21187 headers predicted
 736 pure ACKs
 80497 pure ACKs predicted
UDP:
 139468 datagrams received
 139468 datagrams sent
UDPLite:

```

Table 16-5: Parameters in the output of the **show ip traffic** command

| Parameter                      | Description                    |
|--------------------------------|--------------------------------|
| IPv4                           | IPv4 counters                  |
| IPv6                           | IPv6 counters                  |
| received packets with no route | Received packets with no route |
| truncated packets received     | Truncated packets received     |
| multicast packets received     | Multicast packets received     |
| multicast packets sent         | Multicast packets sent         |
| broadcast packets received     | Broadcast packets received     |
| broadcast packets sent         | Broadcast packets sent         |
| bytes received                 | Bytes received                 |
| bytes sent                     | Bytes sent                     |

Table 16-5: Parameters in the output of the **show ip traffic** command (cont.)

| Parameter                                     | Description                                   |
|-----------------------------------------------|-----------------------------------------------|
| multicast bytes received                      | Multicast bytes received                      |
| multicast bytes sent                          | Multicast bytes sent                          |
| broadcast bytes received                      | Broadcast bytes received                      |
| broadcast bytes sent                          | Broadcast bytes sent                          |
| packets received                              | Packets received                              |
| packets received with invalid headers         | Packets received with invalid headers         |
| oversize packets received                     | Oversize packets received                     |
| packets received with no route                | Packets received with no route                |
| packets received with invalid address         | Packets received with invalid address         |
| packets received with unknown protocol        | Packets received with unknown protocol        |
| truncated packets received                    | Truncated packets received                    |
| received packets discarded                    | Received packets discarded                    |
| received packets delivered                    | Received packets delivered                    |
| forwarded packets transmitted                 | Forwarded packets transmitted                 |
| packets transmitted                           | Packets transmitted                           |
| packets discarded on transmit                 | Packets discarded on transmit                 |
| packets discarded on transmit due to no route | Packets discarded on transmit due to no route |
| fragment reassembly timeouts                  | Fragment reassembly timeouts                  |
| fragment reassembly required                  | Fragment reassembly required                  |
| fragment reassembly OK                        | Fragment reassembly OK                        |
| fragment reassembly failures                  | Fragment reassembly failures                  |
| fragmentations succeeded                      | Fragmentations succeeded                      |
| fragmentations failed                         | Fragmentations failed                         |
| fragments created                             | Fragments created                             |
| ICMP6                                         | ICMPv6 counters                               |
| messages received                             | Messages received                             |
| errors received                               | Errors received                               |
| messages sent                                 | Messages sent                                 |
| TCP                                           | TCP counters                                  |
| remote connections established                | Remote connections established                |

Table 16-5: Parameters in the output of the **show ip traffic** command (cont.)

| Parameter                                    | Description                                                             |
|----------------------------------------------|-------------------------------------------------------------------------|
| local connections established                | Local connections established                                           |
| remote listening ports                       | Remote listening ports                                                  |
| local listening ports                        | Local listening ports                                                   |
| active connection openings                   | Active connection openings                                              |
| passive connection openings                  | Passive connection openings                                             |
| connection attempts failed                   | Connection attempts failed                                              |
| connection resets received                   | Connection resets received                                              |
| segments received                            | Segments received                                                       |
| segments transmitted                         | Segments transmitted                                                    |
| retransmits                                  | Retransmits                                                             |
| bad segments received                        | Bad segments received                                                   |
| resets transmitted                           | Resets transmitted                                                      |
| datagrams received                           | Datagrams received                                                      |
| received for unknown port                    | Received for unknown port                                               |
| datagrams sent                               | Datagrams sent                                                          |
| syncookies sent                              | Syncookies sent                                                         |
| syncookies received                          | Syncookies received                                                     |
| syncookies failed                            | Syncookies failed                                                       |
| embryonic resets                             | Embryonic resets                                                        |
| sockets pruned                               | Sockets pruned                                                          |
| ICMPs out of window                          | ICMPs out of window                                                     |
| ICMPs dropped due to lock                    | ICMPs dropped due to lock                                               |
| ARPs filtered                                | ARPs filtered                                                           |
| TCP sockets finished time wait in fast timer | TCP sockets finished time wait in fast timer                            |
| time wait sockets recycled by time stamp     | Time wait sockets recycled by time stamp                                |
| time wait sockets killed                     | Time wait sockets killed                                                |
| delayed acks sent                            | Delayed acks sent delayed acks further delayed because of locked socket |
| delayed acks lost                            | Delayed acks lost                                                       |
| listening socket overflows                   | Listening socket overflows                                              |
| listening socket drops                       | Listening socket drops                                                  |
| headers predicted                            | Headers predicted                                                       |

Table 16-5: Parameters in the output of the **show ip traffic** command (cont.)

| Parameter                                 | Description                               |
|-------------------------------------------|-------------------------------------------|
| pure ACKs                                 | Pure ACKs                                 |
| pure ACKs predicted                       | Pure ACKs predicted                       |
| losses recovered by TCP Reno              | Losses recovered by TCP Reno              |
| losses recovered by SACK                  | Losses recovered by SACK                  |
| SACKs renegged                            | SACKs renegged                            |
| detected reordering by FACK               | Detected reordering by FACK               |
| detected reordering by SACK               | Detected reordering by SACK               |
| detected reordering by TCP Reno           | Detected reordering by TCP Reno           |
| detected reordering by sequence           | Detected reordering by sequence           |
| full undos                                | Full undos                                |
| partial undos                             | Partial undos                             |
| SACK undos                                | SACK undos                                |
| loss undos                                | Loss undos                                |
| segments lost                             | Segments lost                             |
| lost retransmits                          | Lost retransmits                          |
| TCP Reno failures                         | TCP Reno failures                         |
| SACK failures                             | SACK failures                             |
| loss failures                             | Loss failures                             |
| fast retransmits                          | Fast retransmits                          |
| forward retransmits                       | Forward retransmits                       |
| retransmits in slow start                 | Retransmits in slow start                 |
| timeouts                                  | Timeouts                                  |
| TCP Reno recovery failures                | TCP Reno recovery failures                |
| SACK recovery failures                    | SACK recovery failures                    |
| collapsed segments received               | Collapsed segments received               |
| DSACKs sent for old packets               | DSACKs sent for old packets               |
| DSACKs sent for out of order segments     | DSACKs sent for out of order segments     |
| DSACKs received                           | DSACKs received                           |
| DSACKs received for out of order segments | DSACKs received for out of order segments |
| connections reset due to unexpected SYN   | Connections reset due to unexpected SYN   |



Table 16-5: Parameters in the output of the **show ip traffic** command (cont.)

| Parameter                                   | Description                                 |
|---------------------------------------------|---------------------------------------------|
| connections reset due to unexpected data    | Connections reset due to unexpected data    |
| connections reset due to early user close   | Connections reset due to early user close   |
| connections aborted due to lack of memory   | Connections aborted due to lack of memory   |
| connections aborted due to timeout          | Connections aborted due to timeout          |
| connections aborted due to lingering        | Connections aborted due to lingering        |
| connection aborts due to connection failure | Connection aborts due to connection failure |
| TCP memory pressure events                  | TCP memory pressure events                  |
| SACKs discarded                             | SACKs discarded                             |
| Old DSACKs ignored                          | Old DSACKs ignored                          |
| DSACKs ignored without undo                 | DSACKs ignored without undo                 |
| Spurious RTOs                               | Spurious RTOs                               |
| TCP MD5 Not Found                           | TCP MD5 Not Found                           |
| TCP MD5 Unexpected                          | TCP MD5 Unexpected                          |
| TCP SACKs shifted                           | TCP SACKs shifted                           |
| TCP SACKs merged                            | TCP SACKs merged                            |
| TCP SACK shift fallback                     | TCP SACK shift fallback                     |
| UDP                                         | UDP Counters                                |
| UDPLite                                     | UDPLite Counters                            |
| UDP6                                        | UDPv6 Counters                              |
| UDPLite6                                    | UDPLitev6 Counters                          |
| datagrams received                          | Datagrams received                          |
| datagrams received for unknown port         | Datagrams received for unknown port         |
| datagram receive errors                     | Datagram receive errors                     |
| datagrams transmitted                       | Datagrams transmitted                       |
| datagrams received                          | Datagrams received                          |
| datagrams received for unknown port         | Datagrams received for unknown port         |
| datagram receive errors                     | Datagram receive errors                     |
| datagrams transmitted                       | Datagrams transmitted                       |

# tcpdump

**Overview** GW, Feb 2015 AR3040S and AR4050S don't support VRF Lite for 5.4.5 GA.  
Use this command to start a tcpdump, which gives the same output as the Unix-like **tcpdump** command to display TCP/IP traffic. Press <ct r l> + 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 <a href="http://www.tcpdump.org/tcpdump_man.html">http://www.tcpdump.org/tcpdump_man.html</a> |

**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](#)

# traceroute

**Overview** Use this command to trace the route to the specified IPv4 host.

**Syntax** `traceroute {<ip-addr>|<hostname>}`

| Parameter                     | Description                                                             |
|-------------------------------|-------------------------------------------------------------------------|
| <code>&lt;ip-addr&gt;</code>  | The destination IPv4 address. The IPv4 address uses the format A.B.C.D. |
| <code>&lt;hostname&gt;</code> | The destination hostname.                                               |

**Mode** User Exec and Privileged Exec

**Example** `awplus# traceroute 10.10.0.5`

# undebug ip packet interface

**Overview** This command applies the functionality of the no [debug ip packet interface](#) command.



# 17

# 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](#).

IPv6 is supported in Software Version 5.4.3A-1.x and later.

- Command List**
- “[clear ipv6 neighbors](#)” on page 583
  - “[ipv6 address](#)” on page 584
  - “[ipv6 address autoconfig](#)” on page 585
  - “[ipv6 enable](#)” on page 587
  - “[ipv6 nd raguard](#)” on page 589
  - “[ipv6 neighbor](#)” on page 591
  - “[ipv6 route](#)” on page 592
  - “[ping ipv6](#)” on page 593
  - “[show ipv6 interface brief](#)” on page 594
  - “[show ipv6 neighbors](#)” on page 595
  - “[show ipv6 route](#)” on page 596
  - “[show ipv6 route summary](#)” on page 598
  - “[traceroute ipv6](#)” on page 599

# 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

# ipv6 address

**Overview** Use this command to set the IPv6 address of a VLAN interface and enable IPv6.

IPv6 is supported in Software Version 5.4.3A-1.x and later.

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> [eui64]`  
`no ipv6 address <ipv6-addr/prefix-length>`

| Parameter                                    | Description                                                                                                                                       |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-addr/prefix-length&gt;</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 a VLAN interface.

**Examples** To assign the IPv6 address 2001:0db8::a2/64 to the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

**Validation Commands** `show running-config`  
`show ipv6 interface brief`  
`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 a VLAN interface.

**Usage** 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. When applying SLAAC to an interface, note that the MAC address of the default VLAN is applied to the interface if the interface does not have its own MAC address.

Note that link-local addresses are retained in the system until they are negated by using the **no** variant of the command that established them. See the [ipv6 enable](#) command for more information.

Also note that the link-local address is retained in the system if the global address is removed using another command that was not 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 the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address autoconfig
```

To disable SLAAC on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address autoconfig
```

**Validation  
Commands** [show running-config](#)  
[show ipv6 interface brief](#)  
[show ipv6 route](#)

**Related  
Commands**    [ipv6 address](#)  
                  [ipv6 enable](#)

# ipv6 enable

**Overview** Use this command to enable IPv6 on an interface without an IPv6 global address for the interface. This enables IPv6 with a IPv6 link-local address, not an IPv6 global address.

Use the no variant of this command to disable IPv6 on an interface without a global address. Note the no variant of this command does not operate on an interface with an IPv6 global address or an interface configured for IPv6 stateless address autoconfiguration (SLAAC),

**Syntax** `ipv6 enable`  
`no ipv6 enable`

**Mode** Interface Configuration for a VLAN interface.

**Usage** 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 link-local addresses are retained in the system until they are negated by using the no variant of the command that established them.

Also note that the link-local address is retained in the system if the global address is removed using another command that was not 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 IPv6 with only a link-local IPv6 address on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 enable
```

**Validation  
Commands** `show running-config`  
`show ipv6 interface brief`  
`show ipv6 route`

**Related  
Commands**    [ipv6 address](#)  
[ipv6 address autoconfig](#)

# ipv6 nd raguard

**Overview** Use this command to apply the Router Advertisements (RA) Guard feature from the Interface Configuration mode for a device port. This blocks all RA messages received on a device port.

For more information about RA Guard, see the [IPv6 Feature Overview and Configuration Guide](#).

Use the **no** parameter with this command to disable RA Guard for a specified device port.

**Syntax** `ipv6 nd raguard`  
`no ipv6 nd raguard`

**Default** RA Guard is not enabled by default.

**Mode** Interface Configuration for a device port interface.

**Usage** Router Advertisements (RAs) are used by Routers to announce themselves on the link. Applying RA Guard to a device port disallows Router Advertisements and redirect messages. RA Guard blocks RAs from untrusted hosts. Blocking RAs stops untrusted hosts from flooding malicious RAs and stops any misconfigured hosts from disrupting traffic on the local network.

Enabling RA Guard on a port blocks RAs from a connected host and indicates the port and host are untrusted. Disabling RA Guard on a port allows RAs from a connected host and indicates the port and host are trusted. Ports and hosts are trusted by default to allow RAs.

**Example** To enable RA Guard on device ports `port1.0.2-1.0.12`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-1.0.12
awplus(config-if)# ipv6 nd raguard
```

To verify RA Guard is enabled on device port interface `port1.0.2`, use the command:

```
awplus# show running-config interface port1.0.2
```

To disable RA Guard on device ports `port1.0.2-1.0.12`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.12
awplus(config-if)# no ipv6 nd raguard
```

When RA Guard is disabled on a device port it is not displayed in **show running-config** output.

**Output** Example output from a **show running-config interface** port1.0.2 to verify RA Guard:

```
!
interface port1.0.2
 switchport mode access

 ipv6 nd raguard
!
```

**Related  
Commands** [show running-config interface](#)

# ipv6 neighbor

**Overview** Use this command to add a static IPv6 neighbor entry.  
Use the **no** variant of this command to remove a specific IPv6 neighbor entry.

**Syntax** `ipv6 neighbor <ipv6-address> <vlan-name> <mac-address> <port-list>`  
`no ipv6 neighbor <ipv6-address> <vlan-name> <port-list>`

| Parameter      | Description                                                                              |
|----------------|------------------------------------------------------------------------------------------|
| <ipv6-address> | Specify the neighbor's IPv6 address in format X:X:X:X:X:X.                               |
| <vlan-name>    | Specify the neighbor's VLAN name.                                                        |
| <mac-address>  | Specify the MAC hardware address in hexadecimal notation with the format HHHH.HHHH.HHHH. |
| <port-list>    | Specify the port number, or port range.                                                  |

**Mode** Global Configuration

**Usage** Use this command to clear a specific IPv6 neighbor entry. To clear all dynamic address entries, use the [clear ipv6 neighbors](#) command.

**Example** To create a static neighbor entry for IPv6 address 2001:0db8::a2, on vlan 4, MAC address 0000.cd28.0880, on port 1.0.6, use the command:

```
awplus# configure terminal
awplus(config)# ipv6 neighbor 2001:0db8::a2 vlan4
0000.cd28.0880 port1.0.6
```

**Related Commands** [clear ipv6 neighbors](#)

# ipv6 route

**Overview** Use this command to establish the distance for static routes of a network prefix.

Use the **no** variant of this command to disable the distance for static routes of the network prefix.

**Syntax** `ipv6 route <dest-prefix> <dest-prefix/length>  
{<gateway-ip>|<gateway-name>} [<distvalue>]`

`no ipv6 route <dest-prefix> <dest-prefix/length>  
{<gateway-ip>|<gateway-name>} [<distvalue>]`

| Parameter                               | Description                                                                                                                                                 |
|-----------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;dest-prefix/length&gt;</code> | Specifies the IP destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.        |
| <code>&lt;gateway-ip&gt;</code>         | Specifies the IP gateway (or next hop) address. The IPv6 address uses the format X:X::X/X/Prefix-Length. The prefix-length is usually set between 0 and 64. |
| <code>&lt;distvalue&gt;</code>          | Specifies the administrative distance for the route. Valid values are from 1 to 255.                                                                        |
| <code>&lt;gateway-name&gt;</code>       | Specifies the name of the gateway (or next hop) interface.                                                                                                  |

**Mode** Global Configuration

**Example** `awplus# configure terminal`  
`awplus(config)# ipv6 route myintname 322001:0db8::1/128`

**Validation Commands** `show running-config`  
`show ipv6 route`



# ping ipv6

**Overview** This command sends a query to another IPv6 host (send Echo Request messages).

**NOTE:** Use of the *interface* parameter keyword, plus an interface or an interface range, with this command is only valid when pinging an IPv6 link local address.

**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.                                                         |
| 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.                                                                                                                                                     |
| 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 interface brief

**Overview** Use this command to display brief information about interfaces and the IPv6 address assigned to them.

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 ipv6 interface [brief]

| Parameter | Description                                                                  |
|-----------|------------------------------------------------------------------------------|
| brief     | Specify this optional parameter to display brief IPv6 interface information. |

**Mode** User Exec and Privileged Exec

**Examples** awplus# show ipv6 interface brief

**Output** Figure 17-1: Example output from the **show ipv6 interface brief** command

|                                  |                             |          |          |
|----------------------------------|-----------------------------|----------|----------|
| awplus#show ipv6 interface brief |                             |          |          |
| Interface                        | IPv6-Address                | Status   | Protocol |
| lo                               | unassigned                  | admin up | running  |
| vlan1                            | 2001:db8::1/48              | admin up | down     |
|                                  | fe80::215:77ff:fee9:5c50/64 |          |          |

**Related Commands** [show interface brief](#)

# show ipv6 neighbors

**Overview** Use this command to display all IPv6 neighbors.

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 ipv6 neighbors

**Mode** User Exec and Privileged Exec

# 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show ipv6 route  
[connected|database|summary|<ipv6-address>|<ipv6-addr/prefix-length>)]

| Parameter            | Description                                                                                                                                                                        |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| connected            | Displays only the routes learned from connected interfaces.                                                                                                                        |
| database             | Displays only the IPv6 routing information extracted from the database.                                                                                                            |
| summary              | Displays summary information from the IPv6 routing table.                                                                                                                          |
| <ipv6-address>       | Displays the routes for the specified address in the IP routing table. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64. |
| <ipv6-prefix/length> | Displays only the routes for the specified IP prefix.                                                                                                                              |

**Mode** User Exec and Privileged Exec

**Example 1** To display an IP route with all parameters turned on, use the following command:  
awplus# show ipv6 route

**Output** Figure 17-2: Example output of the **show ipv6 route** command

```
IPv6 Routing Table
Codes: C - connectedS ::/0 [1/0] via 2001::a:0:0:c0a8:a6, vlan10
C 2001:db8::a:0:0:0:0/64 via ::, vlan10
C 2001:db8::14:0:0:0:0/64 via ::, vlan20
C 2001:db8::0:0:0:0:0/64 via ::, vlan30
C 2001:db8::28:0:0:0:0/64 via ::, vlan40
C 2001:db8::fa:0:0:0:0/64 via ::, vlan250
C 2001:db8::/64 via ::, vlan250
C 2001:db8::/64 via ::, vlan40
C 2001:db8::/64 via ::, vlan20
C 2001:db8::/64 via ::, vlan10
```

**Example 2** To display all database entries for an IP route, use the following command:

```
awplus# show ipv6 route database
```

**Output** Figure 17-3: Example output of the **show ipv6 route database** command

```
IPv6 Routing Table
Codes: C - connected> - 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 “Controlling “show” Command Output” in 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 17-4: 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
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>&lt;ipv6-addr&gt;</code> | The destination IPv6 address. The IPv6 address uses the format X:X::X:X. |
| <code>&lt;hostname&gt;</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](#)

# 18

# Static Routing Commands for Management Purposes

## Introduction

**Overview** This chapter provides an alphabetical reference of static routing commands that are used to direct management packets to appropriate VLANs.

- Command List**
- “[ip route](#)” on page 601
  - “[show ip route](#)” on page 602
  - “[show ip route database](#)” on page 604
  - “[show ip route summary](#)” on page 605



# ip route

**Overview** This command lets you create a static route, in order to send management packets to the appropriate VLAN.

Your switch does not use static routes to route traffic from one VLAN to another VLAN, even if the VLANs have IP addresses. You cannot create static routes to route data, only management packets.

The **no** variant of this command removes the static route.

**Syntax** `ip route <subnet&mask> {<gateway-ip>|<interface>} [<distance>]`  
`no ip route <subnet&mask> {<gateway-ip>|<interface>} [<distance>]`

| 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 VLAN interface that the target packets should be sent to. Enter the name of the VLAN or its VID. The gateway IP address or the interface is required. |
| <distance>    | The administrative distance for the static route in the range <1 - 255>. Static routes by default have an administrative distance of 1.                   |

**Mode** Global Configuration

**Default** The default administrative distance for a static route is 1.

**Example** To send management traffic on the 10.0.0.0 network to vlan10 and other management traffic to vlan5, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 10.0.0.0/8 vlan10
awplus(config)# ip route 0.0.0.0/0 vlan5
```

**Related Commands** [show ip route](#)  
[show ip route database](#)

# 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  
[connected|static|<ip-addr>|<ip-addr/prefix-length>]

| Parameter               | Description                                                                             |
|-------------------------|-----------------------------------------------------------------------------------------|
| connected               | Displays only the routes learned from connected interfaces.                             |
| 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

**Example** To display the static routes in the FIB, use the command:

```
awplus# show ip route static
```

**Output** Each entry in the output from this command has a code preceding it, indicating the source of the routing entry. 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 18-1: Example output from the **show ip route** command

```
Codes: C - connected, S - static, R - RIP 0 - 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 3.3.3.0/24 is directly connected, vlan1
C 10.10.31.0/24 is directly connected, vlan2
C 10.70.0.0/24 is directly connected, vlan4
C 33.33.33.33/32 is directly connected, lo
```

**Connected Route** The Connected route entry consists of:

```
C 10.10.31.0/24 is directly connected, vlan2
```

This route entry denotes:

- Route entries for network 10 . 10 . 31 . 0 / 24 are derived from the IP address of local interface v l a n 2.
- These routes are marked as Connected routes ( C ) and always preferred over routes for the same network learned from other routing protocols.

**Related Commands** [show ip route database](#)

# 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 [connected|static]

| Parameter | Description                                                 |
|-----------|-------------------------------------------------------------|
| connected | Displays only the routes learned from connected interfaces. |
| 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 18-2: Example output from the show ip route database command

```
awplus#show ip route database
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
 > - selected route, * - FIB route, p - stale info

S *> 0.0.0.0/0 [1/0] via 10.34.1.1, vlan1
C *> 10.34.0.0/16 is directly connected, vlan1
S 192.168.2.0/24 [1/0] is directly connected, vlan2 inactive

Gateway of last resort is not set
```

The routes added to the FIB are marked with a \*. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. All unselected routes have neither the \* nor the > symbol.

**Related Commands** [show ip route](#)

# 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 18-3: 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
Total 8
```

**Related Commands** [show ip route](#)  
[show ip route database](#)

# 19

# Multicast Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of generic multicast commands. For commands for particular multicast protocols, see:

- [IGMP Snooping Commands](#).
- [MLD Snooping Commands](#)

**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 ip mroute”](#) on page 608
  - [“clear ip mroute statistics”](#) on page 609
  - [“clear ipv6 mroute”](#) on page 610
  - [“clear ipv6 mroute statistics”](#) on page 611
  - [“debug nsm mcast”](#) on page 612
  - [“debug nsm mcast6”](#) on page 613
  - [“ip mroute”](#) on page 614
  - [“ip multicast forward-first-packet”](#) on page 616
  - [“ip multicast route”](#) on page 617

- ["ip multicast route-limit"](#) on page 619
- ["ip multicast wrong-vif-suppression"](#) on page 620
- ["ip multicast-routing"](#) on page 621
- ["ipv6 multicast route"](#) on page 622
- ["ipv6 multicast route-limit"](#) on page 624
- ["ipv6 multicast-routing"](#) on page 625
- ["multicast"](#) on page 626
- ["show ip mroute"](#) on page 627
- ["show ip mvif"](#) on page 629
- ["show ip rpf"](#) on page 630
- ["show ipv6 mroute"](#) on page 631
- ["show ipv6 mif"](#) on page 633

# clear ip mroute

**Overview** Use this command to delete entries from the IPv4 multicast routing table.

**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 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** When this command is used, the Multicast Routing Information Base (MRIB) clears the IPv4 multicast route entries in its IPv4 multicast route table, and removes the entries from the multicast forwarder. The MRIB sends a “clear” message to the multicast protocols. Each multicast protocol has its own “clear” multicast route command. The protocol-specific “clear” command clears multicast routes from PIM Sparse Mode, and also clears the routes from the MRIB.

**Examples** `awplus# clear ip mroute 225.1.1.1 192.168.3.3`  
`awplus# clear ip mroute *`

**Related Commands** [ip multicast route](#)  
[show ip mroute](#)



# 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                                                            |
|--------------------|------------------------------------------------------------------------|
| *                  | All multicast route entries.                                           |
| <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. |

**Mode** Privileged Exec

**Example** `awplus# clear ip mroute statistics 225.1.1.2 192.168.4.4`  
`awplus# clear ip mroute statistics *`

# 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, for example, if you want to create a static route instead of an existing dynamic route.

**Syntax** `clear ipv6 mroute [*|<ipv6-group-address>  
[<ipv6-source-address>]]`

| 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. |

**Mode** Privileged Exec

**Usage** When this command is used, the Multicast Routing Information Base (MRIB) clears the relevant IPv6 multicast route entries in its IPv6 multicast route table, and removes the entries from the multicast forwarder. The MRIB sends a “clear” message to the multicast protocols. Each multicast protocol has its own “clear” multicast route command.

This command does not remove static routes from the routing table or the configuration. To remove static routes, use the `no` parameter of the command [ipv6 multicast route](#).

**Example** `awplus# clear ipv6 mroute 2001::2 ff08::1`

**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.

**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 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 mcast

**Overview** Use this command to debug IPv4 events in the Multicast Routing Information Base (MRIB).

**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**

```
awplus# configure terminal
awplus(config)# debug nsm mcast all
awplus# configure terminal
awplus(config)# debug nsm mcast fib-msg
awplus# configure terminal
awplus(config)# debug nsm mcast mrt
awplus# configure terminal
awplus(config)# debug nsm mcast mtrace
awplus# configure terminal
awplus(config)# debug nsm mcast mtrace-detail
awplus# configure terminal
awplus(config)# debug nsm mcast register
awplus# configure terminal
awplus(config)# debug nsm mcast stat
awplus# configure terminal
awplus(config)# debug nsm mcast vif
```

# debug nsm mcast6

**Overview** Use this command to debug IPv6 events in the Multicast Routing Information Base (MRIB).

**Syntax** `debug nsm mcast6`  
`{all|fib-msg|mrt|mtrace|mtrace-detail|register|stats|vif}`

| Parameter | Description                                 |
|-----------|---------------------------------------------|
| all       | All IPv4 multicast debugging.               |
| fib-msg   | Forwarding Information Base (FIB) messages. |
| mif       | Multicast interfaces.                       |
| mrt       | Multicast routes.                           |
| register  | Multicast PIM register messages.            |
| stats     | Multicast statistics.                       |

**Mode** Privileged Exec and Global Configuration

**Examples**

```
awplus# configure terminal
awplus(config)# debug nsm mcast6 all
awplus# configure terminal
awplus(config)# debug nsm mcast6 fib-msg
awplus# configure terminal
awplus(config)# debug nsm mcast6 mif
awplus# configure terminal
awplus(config)# debug nsm mcast6 mrt
awplus# configure terminal
awplus(config)# debug nsm mcast6 register
awplus# configure terminal
awplus(config)# debug nsm mcast6 stats
```

# 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>]`  
`no ip mroute <ipv4-source-address/mask-length> [bgp|ospf|rip|static]`

| 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>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** 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** `show ip rpf`

# ip multicast forward-first-packet

**Overview** Use this command to enable multicast to forward the first multicast packets coming to the device.

Use the **no** variant of this command to disable this feature.

**Syntax** `ip multicast forward-first-packet`  
`no ip multicast forward-first-packet`

**Default** By default, this feature is disabled.

**Mode** Global Configuration

**Usage** If this command is enabled, the device will forward the first packets in a multicast stream that create the multicast route, possibly causing degradation in the quality of the multicast stream, such as the pixelation of video and audio data.

**NOTE:** *If you use this command, ensure that the [ip igmp snooping](#) command is enabled, the default setting, otherwise the device will not process the first packets of the multicast stream correctly.*

The device will forward the first multicast packets to all interfaces which are on the same VLAN as those which asked for this multicast group.

**Examples** To enable the forwarding of the first multicast packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast forward-first-packet
```

To disable the forwarding of the first multicast packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast forward-first-packet
```



# 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 VLAN to a single or range of downstream VLANs.

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 VLAN 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-vlan-id> [<downstream-vlan-id>]`  
`no ip multicast route <ipv4-source-addr> <ipv4-group-addr> [<upstream-vlan-id> <downstream-vlan-id>]`

| Parameter                               | Description                                                                                    |
|-----------------------------------------|------------------------------------------------------------------------------------------------|
| <code>&lt;ipv4-source-addr&gt;</code>   | Source IPv4 address, in dotted decimal notation in the format A.B.C.D.                         |
| <code>&lt;ipv4-group-addr&gt;</code>    | Group IPv4 address, in dotted decimal notation in the format A.B.C.D.                          |
| <code>&lt;upstream-vlan-id&gt;</code>   | Upstream VLAN interface on which the multicast packets ingress.                                |
| <code>&lt;downstream-vlan-id&gt;</code> | Downstream VLAN interface or range of VLAN interfaces to which the multicast packets are sent. |

**Default** By default, this feature is disabled.

**Mode** Global Configuration

**Usage** 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 same source IPv4 address, group IPv4 address, upstream VLAN and downstream VLANs. 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 VLANs, you must firstly remove the existing static multicast route and then add the new static multicast route with all downstream VLANs specified. If you attempt to update an existing static multicast route entry with an additional VLAN or VLANs an error message is displayed and logged.

To remove a specific downstream VLAN from an existing static multicast route entry, specify the VLAN you want to remove with the `<downstream-vlan-id>` 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 VLAN interface as `vlan10` and the downstream VLAN interface as `vlan20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11 vlan10
vlan20
```

To create an IPv4 static multicast route for the multicast source IPv4 address `2.2.2.2` and group IP address `224.9.10.11`, specifying the upstream VLAN interface as `vlan10` and the downstream VLAN range as `vlan20-25`, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11 vlan10
vlan20-25
```

To remove the downstream VLAN 23 from the IPv4 static multicast route created with the above command, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast route 2.2.2.2 224.9.10.11
vlan10 vlan23
```

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](#)  
[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** 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`

# ip multicast wrong-vif-suppression

- Overview** Use this command to prevent unwanted multicast packets received on an unexpected VLAN 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** 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** 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`

# 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 ingress on an upstream VLAN to a single or range of downstream VLANs.

See detailed usage notes below to configure static multicast router ports when using static IPv6 multicast routes with EPSR, and the destination VLAN is an EPSR data VLAN.

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 VLAN 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-vlan-id> [<downstream-vlan-id>]`  
`no ipv6 multicast route <ipv6-source-addr> <ipv6-group-addr> [<upstream-vlan-id> <downstream-vlan-id>]`

| Parameter                               | Description                                                                                    |
|-----------------------------------------|------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-group-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-vlan-id&gt;</code>   | Upstream VLAN interface on which the multicast packets ingress.                                |
| <code>&lt;downstream-vlan-id&gt;</code> | Downstream VLAN interface or range of VLAN interfaces to which the multicast packets are sent. |

**Default** By default, no static routes exist.

**Mode** Global Configuration

**Usage** 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 VLANs, you must firstly remove the existing static multicast route and then add the new static multicast route with all downstream VLANs specified. If

you attempt to update an existing static multicast route entry with an additional VLAN or VLANs an error message is displayed and logged.

To remove a specific downstream VLAN from an existing static multicast route entry, specify the VLAN you want to remove with the `<downstream-vlan-id>` parameter when entering the **no** variant of this command.

Note that if static IPv6 multicast routing is being used with EPSR and the destination VLAN is an EPSR data VLAN, then multicast router (mrouter) ports must be statically configured. This minimizes disruption for multicast traffic in the event of ring failure or restoration.

When configuring the EPSR data VLAN, statically configure mrouter ports so that the multicast router can be reached in either direction around the EPSR ring.

See [ipv6 mld snooping mrouter](#) for a command description and command examples.

**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 VLAN interface as `vlan10` and the downstream VLAN interface as `vlan20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast route 2001::1 ff08::1 vlan10
vlan20
```

To create an IPv6 static multicast route for the multicast source IPv6 address 2001::1 and group IPv6 address ff08::1, specifying the upstream VLAN interface as `vlan10` and the downstream VLAN range as `vlan20-25`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast route 2001::1 ff08::1 vlan10
vlan20-25
```

To remove the downstream VLAN 23 from the IPv6 static multicast route created with the above command, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 multicast route 2001::1 ff08::1 vlan10
vlan23
```

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 mld snooping mrouter](#)  
[show 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** 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** `awplus# configure terminal`  
`awplus(config)# ipv6 multicast route-limit 34 24`  
`awplus# configure terminal`  
`awplus(config)# no ipv6 multicast route-limit`



# 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** By default, IPv6 multicast routing is 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** `awplus# configure terminal`  
`awplus(config)# ipv6 multicast-routing`  
`awplus# configure terminal`  
`awplus(config)# no ipv6 multicast-routing`

**Validation Commands** `show running-config`

# multicast

**Overview** Use this command to enable a device port to route multicast packets that ingress the port.

Use the **no** variant of this command to stop the device port from routing multicast packets that ingress the port. Note that this does not affect Layer 2 forwarding of multicast packets. If you enter **no multicast** on a port, multicast packets received on that port will not be forwarded to other VLANs, but ports in the same VLANs as the receiving port will still receive the multicast packets.

**Syntax** multicast  
no multicast

**Default** By default, all device ports route multicast packets.

**Mode** Interface Configuration

**Examples** awplus# configure terminal  
awplus(config-if)# multicast  
awplus# configure terminal  
awplus(config-if)# no multicast

**Validation  
Commands** show running-config

# 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}] [{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.                                                     |
| 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 19-1: 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: vlan2
 Outgoing interface list:
 vlan3 (1)
```

Figure 19-2: 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: vlan2
 Outgoing interface list:
 vlan3 (1)
```

The following is a sample output of this command displaying the packet count from the IPv4 multicast routing table:

Figure 19-3: 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 19-4: 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
```

# 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 vlan2

**Output** Figure 19-5: Example output from the **show ip mvif** command

| Interface | Vif<br>Idx | Owner<br>Module | TTL | Local<br>Address | Remote<br>Address | Uptime   |
|-----------|------------|-----------------|-----|------------------|-------------------|----------|
| vlan2     | 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 |
| vlan3     | 2          | PIM-SM          | 1   | 192.168.10.53    | 0.0.0.0           | 00:04:25 |

Figure 19-6: Example output from the **show ip mvif** command with the interface parameter **vlan2** specified

| Interface | Vif<br>Idx | Owner<br>Module | TTL | Local<br>Address | Remote<br>Address | Uptime   |
|-----------|------------|-----------------|-----|------------------|-------------------|----------|
| vlan2     | 0          | PIM-SM          | 1   | 192.168.1.53     | 0.0.0.0           | 00:05:17 |

# 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                                                            |
|--------------------|------------------------------------------------------------------------|
| <ipv4-source-addr> | 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

# 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 19-7: 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: vlan2
 Outgoing interface list:
 vlan3
```

The following is a sample output of this command displaying the IPv6 multicast routing count table for a single static IPv6 Multicast route:

Figure 19-8: 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 recv 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 recv/Reg NACK recv/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 recv
Client msg counts: WRONGmif/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/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 19-9: 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 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> | The interface to display information about. |

**Mode** User Exec and Privileged Exec

**Example** `awplus# show ipv6 mif`  
`awplus# show ipv6 mif vlan2`

**Output** Figure 19-10: Example output from the **show ipv6 mif** command

```
awplus#show ipv6 mif
```

| Interface | Mif<br>Idx | Owner<br>Module       | Uptime   |
|-----------|------------|-----------------------|----------|
| vlan3     | 0          | MLD/MLD Proxy-Service | 03:28:48 |
| vlan2     | 1          | MLD/MLD Proxy-Service | 03:28:48 |
| vlan1     | 2          | MLD/MLD Proxy-Service | 03:28:48 |

Figure 19-11: Example output from the **show ipv6 mif** command with the interface parameter **vlan2** specified

| Interface | Mif<br>Idx | Owner<br>Module | TTL | Remote<br>Address | Uptime   |
|-----------|------------|-----------------|-----|-------------------|----------|
| vlan2     | 0          | PIM-SMv6        | 1   | 0.0.0.0           | 00:05:17 |

# 20

# IGMP Snooping Commands

## Introduction

**Overview** The Internet Group Management Protocol (IGMP) module includes IGMP Snooping functionality. Some of the following commands may have commonalities and restrictions. These are described under the Usage section for each command.

- Command List**
- [“clear ip igmp”](#) on page 635
  - [“clear ip igmp group”](#) on page 636
  - [“clear ip igmp interface”](#) on page 637
  - [“debug igmp”](#) on page 638
  - [“ip igmp snooping”](#) on page 639
  - [“ip igmp snooping fast-leave”](#) on page 640
  - [“ip igmp snooping querier”](#) on page 641
  - [“ip igmp snooping report-suppression”](#) on page 642
  - [“ip igmp snooping tcn query solicit”](#) on page 643
  - [“ip igmp static-group”](#) on page 645
  - [“ip igmp version”](#) on page 647
  - [“show debugging igmp”](#) on page 648
  - [“show ip igmp groups”](#) on page 649
  - [“show ip igmp interface”](#) on page 651
  - [“show ip igmp snooping statistics”](#) on page 654
  - [“undebug igmp”](#) on page 655

# clear ip igmp

**Overview** Use this command to clear all IGMP group membership records on all VLAN interfaces.

**Syntax** `clear ip igmp`

**Mode** Privileged Exec

**Usage** This command applies to VLAN interfaces configured for IGMP Snooping.

**Example** `awplus# clear ip igmp`

**Validation  
Commands** `show ip igmp interface`  
`show running-config`

**Related  
Commands** `clear ip igmp group`  
`clear ip igmp interface`

# clear ip igmp group

**Overview** Use this command to clear IGMP group membership records for a specific group on either all VLAN interfaces, a single VLAN interface, or for a range of VLAN interfaces.

**Syntax** `clear ip igmp group *`  
`clear ip igmp group <ip-address> <interface>`

| Parameter                       | Description                                                                                                         |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------|
| <code>*</code>                  | Clears all groups on all VLAN interfaces. This is an alias to the <code>clear ip igmp</code> command.               |
| <code>&lt;ip-address&gt;</code> | Specifies the group whose membership records will be cleared from all VLAN interfaces, entered in the form A.B.C.D. |
| <code>&lt;interface&gt;</code>  | Specifies the name of the VLAN interface; all groups learned on this VLAN interface are deleted.                    |

**Mode** Privileged Exec

**Usage** This command applies to groups learned by IGMP Snooping.  
In addition to the group a VLAN interface can be specified. Specifying this will mean that only entries with the group learned on the interface will be deleted.

**Examples** `awplus# clear ip igmp group *`  
`awplus# clear ip igmp group 224.1.1.1 vlan1`

**Validation  
Commands** `show ip igmp interface`  
`show running-config`

**Related  
Commands** `clear ip igmp`  
`clear ip igmp interface`

# clear ip igmp interface

**Overview** Use this command to clear IGMP group membership records on a particular VLAN interface.

**Syntax** clear ip igmp interface *<interface>*

| Parameter                | Description                                                                                      |
|--------------------------|--------------------------------------------------------------------------------------------------|
| <i>&lt;interface&gt;</i> | Specifies the name of the VLAN interface. All groups learned on this VLAN interface are deleted. |

**Mode** Privileged Exec

**Usage** This command applies to interfaces configured for IGMP Snooping.

**Example** awplus# clear ip igmp interface vlan1

**Validation  
Commands** show ip igmp interface  
show running-config

**Related  
Commands** clear ip igmp  
clear ip igmp group

# 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

**Usage** This command applies to interfaces configured for IGMP Snooping.

**Example** `awplus# configure terminal`  
`awplus(config)# debug igmp all`

**Related Commands** [show debugging igmp](#)  
[undebug igmp](#)

# ip igmp snooping

**Overview** Use this command to enable IGMP Snooping. When this command is used in the Global Configuration mode, IGMP Snooping is enabled at the device level. When this command is used in Interface Configuration mode, IGMP Snooping is enabled for the specified VLANs.

Use the **no** variant of this command to either globally disable IGMP Snooping, or disable IGMP Snooping on a specified interface.

**NOTE:** *IGMP snooping cannot be disabled on an interface if IGMP snooping has already been disabled globally. IGMP snooping can be disabled on both an interface and globally if disabled on the interface first and then disabled globally.*

**Syntax** ip igmp snooping  
no ip igmp snooping

**Default** By default, IGMP Snooping is enabled both globally and on all VLANs.

**Mode** Global Configuration and Interface Configuration for a VLAN interface.

**Usage** For IGMP snooping to operate on particular VLAN interfaces, it must be enabled both globally by using this command in Global Configuration mode, and on individual VLAN interfaces by using this command in Interface Configuration mode (both are enabled by default.)

Both IGMP snooping and MLD snooping must be enabled globally on the device for IGMP snooping to operate. MLD snooping is also enabled by default. To enable it if it has been disabled, use the [ipv6 mld snooping](#) command in Global Configuration mode.

**Examples** awplus# configure terminal  
awplus(config)# ip igmp snooping  
awplus# configure terminal  
awplus(config)# interface vlan2  
awplus(config-if)# ip igmp snooping

**Related Commands** [ipv6 mld snooping](#)  
[show ip igmp interface](#)  
[show running-config](#)

## ip igmp snooping fast-leave

**Overview** Use this command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing. The IGMP group-membership entry is removed as soon as an IGMP leave group message is received, without sending out a group-specific query.

Use the **no** variant of this command to disable fast-leave processing.

**Syntax** `ip igmp snooping fast-leave`  
`no ip igmp snooping fast-leave`

**Default** IGMP Snooping fast-leave processing is disabled.

**Mode** Interface Configuration for a VLAN interface.

**Usage** This IGMP Snooping command can only be configured on VLAN interfaces.

**Example** This example shows how to enable fast-leave processing on the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping fast-leave
```

**Validation  
Commands** `show ip igmp interface`  
`show running-config`



# ip igmp snooping querier

**Overview** Use this command to enable IGMP querier operation when no multicast routing protocol is configured. When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces. This command applies to interfaces configured for IGMP Snooping.

Use the **no** variant of this command to disable IGMP querier configuration.

**Syntax** `ip igmp snooping querier`  
`no ip igmp snooping querier`

**Mode** Interface Configuration for a VLAN interface.

**Usage** The IGMP Snooping querier uses the 0.0.0.0 Source IP address because it only masquerades as a proxy IGMP querier for faster network convergence.

It does not start, or automatically cease, the IGMP Querier operation if it detects query message(s) from a multicast router.

If an IP address is assigned to a VLAN, which has IGMP querier enabled on it, then the IGMP Snooping querier uses the VLAN's IP address as the Source IP Address in IGMP queries.

The IGMP Snooping Querier will not stop sending IGMP Queries if there is another IGMP Snooping Querier in the network with a lower Source IP Address.

**NOTE:** Do not enable the IGMP Snooping Querier feature on a Layer 2 device when there is an operational IGMP Querier in the network.

**Example** `awplus# configure terminal`  
`awplus(config)# interface vlan2`  
`awplus(config-if)# ip igmp snooping querier`

**Validation  
Commands** `show ip igmp interface`  
`show running-config`

# ip igmp snooping report-suppression

**Overview** Use this command to enable report suppression for IGMP versions 1 and 2. This command applies to interfaces configured for IGMP Snooping.

Report suppression stops reports being sent to an upstream multicast router port when there are already downstream ports for this group on this interface.

Use the **no** variant of this command to disable report suppression.

**Syntax** `ip igmp snooping report-suppression`  
`no ip igmp snooping report-suppression`

**Default** Report suppression does not apply to IGMPv3, and is turned on by default for IGMPv1 and IGMPv2 reports.

**Mode** Interface Configuration for a VLAN interface.

**Example** This example shows how to enable report suppression for IGMPv2 reports for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp version 2
awplus(config-if)# ip igmp snooping report-suppression
```

**Validation  
Commands** `show ip igmp interface`  
`show running-config`

# ip igmp snooping tcn query solicit

**Overview** Use this command to enable IGMP (Internet Group Management Protocol) Snooping TCN (Topology Change Notification) Query Solicitation feature. When this command is used in the Global Configuration mode, Query Solicitation is enabled.

Use the **no** variant of this command to disable IGMP Snooping TCN Query Solicitation. When the no variant of this command is used in Interface Configuration mode, this overrides the Global Configuration mode setting and Query Solicitation is disabled.

**Syntax** ip igmp snooping tcn query solicit  
no ip igmp snooping tcn query solicit

**Default** IGMP Snooping TCN Query Solicitation is disabled by default on the device, unless the device is the Master Node in an EPSR ring, or is the Root Bridge in a Spanning Tree.

When the device is the Master Node in an EPSR ring, or the device is the Root Bridge in a Spanning Tree, then IGMP Snooping TCN Query Solicitation is enabled by default and cannot be disabled using the Global Configuration mode command. However, Query Solicitation can be disabled for specified VLANs using this command from the Interface Configuration mode. Select the VLAN you want to disable in Interface Configuration mode then issue the no variant of this command to disable the specified VLAN without disabling this feature for other VLANs.

**Mode** Global Configuration and Interface Configuration for a VLAN interface.

**Usage** Once enabled, if the device is not an IGMP Querier, on detecting a topology change, the device generates IGMP Query Solicit messages that are sent to all the ports of the vlan configured for IGMP Snooping on the device.

On a device that is not the Master Node in an EPSR ring or the Root Bridge in a Spanning Tree, Query Solicitation can be disabled using the **no** variant of this command after being enabled.

If the device that detects a topology change is an IGMP Querier then the device will generate an IGMP Query message.

Note that the **no** variant of this command when issued in Global Configuration mode has no effect on a device that is the Master Node in an EPSR ring or on a device that is a Root Bridge in a Spanning Tree. Query Solicitation is not disabled for the device these instances. However, Query Solicitation can be disabled on a per-vlan basis from the Interface Configuration mode.

See the below state table that shows when Query Solicit messages are sent in these instances:

| Command issued from Global Configuration | Device is STP Root Bridge or the EPSR Master Node | Command issued from Interface Configuration | IGMP Query Solicit message sent on VLAN |
|------------------------------------------|---------------------------------------------------|---------------------------------------------|-----------------------------------------|
| No                                       | Yes                                               | Yes                                         | Yes                                     |
| Yes                                      | Yes                                               | No                                          | No                                      |
| Yes                                      | Yes                                               | Yes                                         | Yes                                     |

See the [IGMP Feature Overview and Configuration Guide](#) for introductory information about the Query Solicitation feature.

**Examples** This example shows how to enable IGMP Snooping TCN Query Solicitation on a device:

```
awplus# configure terminal
awplus(config)# ip igmp snooping tcn query solicit
```

This example shows how to disable IGMP Snooping TCN Query Solicitation on a device:

```
awplus# configure terminal
awplus(config)# no ip igmp snooping tcn query solicit
```

This example shows how to enable IGMP Snooping TCN Query Solicitation for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping tcn query solicit
```

This example shows how to disable IGMP Snooping TCN Query Solicitation for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip igmp snooping tcn query solicit
```

**Validation Commands** [show ip igmp interface](#)  
[show running-config](#)

## ip igmp static-group

**Overview** Use this command to statically configure multicast group membership entries on a VLAN interface, or to statically forward a multicast channel out a particular port or port range.

To statically add only a group membership, do not specify any parameters.

To statically add a (\*,g) entry to forward a channel out of a port, specify only the multicast group address and the switch port range.

To statically add an (s,g) entry to forward a channel out of a port, specify the multicast group address, the source IP address, and the switch port range.

Use the **no** variant of this command to delete static group membership entries.

**Syntax** `ip igmp static-group <ip-address> [source {<ip-source-addr>}] [interface <port>]`  
`no ip igmp static-group <ip-address> [source {<ip-source-addr>}] [interface <port>]`

| Parameter        | Description                                                                                                                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-address>     | Standard IP Multicast group address, entered in the form A.B.C.D, to be configured as a static group member.                                                                                       |
| source           | Optional.                                                                                                                                                                                          |
| <ip-source-addr> | Standard IP source address, entered in the form A.B.C.D, to be configured as a static source from where multicast packets originate.                                                               |
| interface        | Use this parameter to specify a specific switch port or switch port range to statically forward the multicast group out of. If not used, static configuration is applied on all ports in the VLAN. |
| <port>           | The port or port range to statically forward the group out of. The port may be a switch port (e.g. port 1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2).   |

**Mode** Interface Configuration for a VLAN interface.

**Usage** This command applies to IGMP Snooping on a VLAN interface, to statically add group and/ or source records.

**Example** The following example show how to statically add group and source records for IGMP on the VLAN interface vlan3:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip igmp
awplus(config-if)# ip igmp static-group 226.1.2.4 source
10.2.3.4
```

## 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                  |
|-----------|------------------------------|
| <1-3>     | IGMP protocol version number |

**Default** The default IGMP protocol version number is 3.

**Mode** Interface Configuration for a VLAN interface.

**Usage** This command applies to VLAN interfaces configured for IGMP.

**Example** `awplus# configure terminal`  
`awplus(config)# interface vlan5`  
`awplus(config-if)# ip igmp version 2`

**Validation  
Commands** `show ip igmp interface`

# show debugging igmp

**Overview** Use this command to display the IGMP debugging options set.  
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 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 20-1: 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](#)



# 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show ip igmp groups [<ip-address>|<interface> 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.       |

**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 20-2: Example output from the **show ip igmp groups** command

| IGMP Connected Group Membership |           |          |          |               |  |
|---------------------------------|-----------|----------|----------|---------------|--|
| Group Address                   | Interface | Uptime   | Expires  | Last Reporter |  |
| 224.0.1.1                       | port1.0.1 | 00:00:09 | 00:04:17 | 10.10.0.82    |  |
| 224.0.1.24                      | port1.0.2 | 00:00:06 | 00:04:14 | 10.10.0.84    |  |
| 224.0.1.40                      | port1.0.3 | 00:00:09 | 00:04:15 | 10.10.0.91    |  |
| 224.0.1.60                      | port1.0.3 | 00:00:05 | 00:04:15 | 10.10.0.7     |  |
| 224.100.100.100                 | port1.0.1 | 00:00:11 | 00:04:13 | 10.10.0.91    |  |
| 228.5.16.8                      | port1.0.3 | 00:00:11 | 00:04:16 | 10.10.0.91    |  |
| 228.81.16.8                     | port1.0.6 | 00:00:05 | 00:04:15 | 10.10.0.91    |  |
| 228.249.13.8                    | port1.0.3 | 00:00:08 | 00:04:17 | 10.10.0.91    |  |
| 235.80.68.83                    | port1.0.5 | 00:00:12 | 00:04:15 | 10.10.0.40    |  |
| 239.255.255.250                 | port1.0.3 | 00:00:12 | 00:04:15 | 10.10.0.228   |  |
| 239.255.255.254                 | port1.0.4 | 00:00:08 | 00:04:13 | 10.10.0.84    |  |

Table 20-1: Parameters in the output of the **show ip igmp groups** command

| Parameter     | Description                                |
|---------------|--------------------------------------------|
| Group Address | Address of the multicast group.            |
| Interface     | Port through which the group is reachable. |

Table 20-1: Parameters in the output of the **show ip igmp groups** command

| Parameter     | Description                                                                                                  |
|---------------|--------------------------------------------------------------------------------------------------------------|
| Uptime        | The time in weeks, days, hours, minutes, and seconds that this multicast group has been known to the device. |
| Expires       | Time (in hours, minutes, and seconds) until the entry expires.                                               |
| Last Reporter | Last host to report being a member of the multicast group.                                                   |

# show ip igmp interface

**Overview** Use this command to display the state of IGMP Snooping for a specified VLAN, or all VLANs. IGMP is shown as Active or Disabled in the show output.

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 ip igmp interface [<interface>]

| Parameter   | Description                     |
|-------------|---------------------------------|
| <interface> | The name of the VLAN interface. |

**Mode** User Exec and Privileged Exec

**Examples** The following output shows IGMP interface status for **vlan2** (with IGMP Snooping enabled):

```
awplus#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
awplus(config)#interface vlan2
awplus(config-if)#ip igmp snooping
awplus(config-if)#exit
awplus(config)#exit
awplus#show ip igmp interface vlan2
Interface vlan2 (Index 202)
 IGMP Disabled, Inactive, Version 3 (default)
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 Source Address checking is enabled
IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally disabled
 Num. query-solicit packets: 57 sent, 0 recvd
IGMP Snooping is enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
awplus#
```

The following output shows IGMP interface status for **vlan2** (with IGMP Snooping disabled):

```
awplus#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
awplus(config)#interface vlan2
awplus(config-if)#no ip igmp snooping
awplus(config-if)#exit
awplus(config)#exit
awplus#show ip igmp interface vlan2
Interface vlan2 (Index 202)
 IGMP Disabled, Inactive, Version 3 (default)
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 Source Address checking is enabled
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally disabled
 Num. query-solicit packets: 57 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
awplus#
```

The following command displays the IGMP interface status and Query Solicitation for **vlan3**:

```
awplus#show ip igmp interface vlan3
Interface vlan3 (Index 203)
 IGMP Enabled, Active, Querier, Version 3 (default)
 Internet address is 192.168.9.1
 IGMP interface has 256 group-record states
 IGMP activity: 51840 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 250 seconds
 IGMP max query response time is 1 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 251 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally enabled
 Num. query-solicit packets: 1 sent, 10 recvd
 IGMP Snooping is enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
awplus#
```

**NOTE:** Query Solicitation status information is highlighted in **bold** in the above output.

Use the **show ip igmp interface** command to validate that Query Solicitation is enabled and to show the number of query-solicit message packets sent and received on a VLAN.

**Related  
Commands**

clear ip igmp  
clear ip igmp group  
clear ip igmp interface  
ip igmp snooping  
ip igmp snooping fast-leave  
ip igmp snooping querier  
ip igmp snooping report-suppression  
ip igmp snooping tcn query solicit  
ip igmp version

# show ip igmp snooping statistics

**Overview** Use this command to display IGMP Snooping statistics data.

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 ip igmp snooping statistics interface <interface-range> [group [<ip-address>]]`

| Parameter    | Description                                                                         |
|--------------|-------------------------------------------------------------------------------------|
| <ip-address> | Optionally specify the address of the multicast group, entered in the form A.B.C.D. |
| <interface>  | Specify the name of the VLAN interface or interface range.                          |

**Mode** User Exec and Privileged Exec

**Example** To display IGMP statistical information for **vlan1** and **vlan2**, use the command:

```
awplus# show ip igmp snooping statistics interface vlan1-vlan2
```

**Output** Figure 20-3: Example output from the **show ip igmp snooping statistics** command

```
IGMP Snooping statistics for vlan1
Interface: port1.0.3
Group: 224.1.1.1
Uptime: 00:00:09
Group mode: Exclude (Expires: 00:04:10)
Last reporter: 10.4.4.5
Source list is empty
IGMP Snooping statistics for vlan2
Interface: port1.0.4
Group: 224.1.1.2
Uptime: 00:00:19
Group mode: Exclude (Expires: 00:05:10)
Last reporter: 10.4.4.6
Source list is empty
```

# undebbug igmp

**Overview** This command applies the functionality of the no [debug igmp](#) command.

# 21

# MLD Snooping Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of configuration, clear, and show commands related to MLD Snooping.

**NOTE:**

- Command List**
- “clear ipv6 mld” on page 657
  - “clear ipv6 mld group” on page 658
  - “clear ipv6 mld interface” on page 659
  - “debug mld” on page 660
  - “ipv6 mld access-group” on page 661
  - “ipv6 mld limit” on page 662
  - “ipv6 mld snooping” on page 664
  - “ipv6 mld snooping fast-leave” on page 666
  - “ipv6 mld snooping mrouter” on page 667
  - “ipv6 mld snooping querier” on page 669
  - “ipv6 mld snooping report-suppression” on page 670
  - “ipv6 mld static-group” on page 672
  - “show debugging mld” on page 674
  - “show ipv6 mld groups” on page 675
  - “show ipv6 mld interface” on page 676
  - “show ipv6 mld snooping mrouter” on page 677
  - “show ipv6 mld snooping statistics” on page 678



# clear ipv6 mld

**Overview** Use this command to clear all MLD local memberships on all interfaces.

**Syntax** `clear ipv6 mld`

**Mode** Privileged Exec

**Example** `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 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** `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                                                                          |
|-------------|--------------------------------------------------------------------------------------|
| <interface> | Specifies name of the interface; all groups learned from this interface are deleted. |

**Mode** Privileged Exec

**Example** `awplus# clear ipv6 mld interface vlan2`

**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 access-group

**Overview** Use this command to control the multicast local-membership groups learned on an interface.

Use the **no** variant of this command to disable this access control.

**Syntax** `ipv6 mld access-group <IPv6-access-list-name>`  
`no ipv6 mld access-group`

| Parameter                                  | Description                                                                                                                                                     |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;IPv6-access-list-name&gt;</code> | Specify a Standard or an Extended software IPv6 access-list name. See <a href="#">IPv6 Software Access Control List (ACL) Commands</a> for supported IPv6 ACLs. |

**Default** No access list is configured by default.

**Mode** Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

**Examples** In the following example, the VLAN interface `vlan2` will only accept MLD joins for groups in the range `ff1e:0db8:0001::/64`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard group1 permit ff1e:0db8:0001::/64
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld access-group group1
```

In the following example, the VLAN interfaces `vlan2-vlan4` will only accept MLD joins for groups in the range `ff1e:0db8:0001::/64`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard group1 permit ff1e:0db8:0001::/64
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld access-group group1
```

# ipv6 mld limit

**Overview** Use this command to configure a limit on the maximum number of group memberships that may be learned. The limit may be set for the device as a whole, or for a specific interface.

Once the specified group membership limit is reached, all further local-memberships will be ignored.

Optionally, an exception access-list can be configured to specify the group-address(es) that are exempted from being subject to the limit.

Use the **no** variant of this command to unset the limit and any specified exception access-list.

**Syntax** `ipv6 mld limit <limitvalue> [except <IPv6-access-list-name>]`  
`no ipv6 mld limit`

| Parameter               | Description                                                                                                                                                                                                                                                     |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <limitvalue>            | <2-512> Maximum number of group membership states.                                                                                                                                                                                                              |
| <IPv6-access-list-name> | Specify a Standard or an Extended software IPv6 access-list name that defines multicast groups, which are exempted from being subject to the configured limit.<br>See <a href="#">IPv6 Software Access Control List (ACL) Commands</a> for supported IPv6 ACLs. |

**Default** The default limit, which is reset by the **no** variant of this command, is the same as maximum number of group membership entries that can be learned with the **ipv6 mld limit** command.

The default limit of group membership entries that can be learned is 512 entries.

**Mode** Global Configuration and Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

**Usage** This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

**Examples** The following example configures an MLD limit of 100 group-memberships across all VLAN interfaces on which MLD is enabled, and excludes groups in the range `ff1e:0db8:0001::/64` from this limitation:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard v6grp permit
ff1e:0db8:0001::/64
awplus(config)# ipv6 mld limit 100 except v6grp
```

The following example configures an MLD limit of 100 group-membership states on the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld limit 100
```

The following example configures an MLD limit of 100 group-membership states on the VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld limit 100
show ipv6 mld groups
```

# ipv6 mld snooping

**Overview** Use this command to enable MLD Snooping. When this command is issued in the Global Configuration mode, MLD Snooping is enabled globally for the device. When this command is issued in Interface mode for a VLAN then MLD Snooping is enabled for the specified VLAN. Note that MLD Snooping is enabled on the VLAN only if it is enabled globally and on the VLAN.

Use the **no** variant of this command to globally disable MLD Snooping in Global Configuration mode, or for the specified VLAN interface in Interface mode.

**NOTE:** *There is a 100 MLD interface limit when applying MLD commands to multiple VLANs. Only the first 100 VLANs have the required multicast structures added to the interfaces that allow multicast routing.*

*The device has a 512 MLD group limit for (\*, G) and (S,G) entries.*

**Syntax** `ipv6 mld snooping`  
`no ipv6 mld snooping`

**Default** By default, MLD Snooping is enabled both globally and on all VLANs.

**Mode** Global Configuration and Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

**Usage** For MLD Snooping to operate on particular VLAN interfaces, it must be enabled both globally by using this command in Global Configuration mode, and on individual VLAN interfaces by using this command in Interface Configuration mode (both are enabled by default).

MLD requires memory for storing data structures, as well as the hardware tables to implement hardware routing. As the number of ports, VLANs, static and dynamic groups increases then more memory is consumed. You can track the memory used for MLD with the command:

```
awplus# show memory pools nsm | grep MLD
```

Static and dynamic groups (LACP), ports and VLANs are not limited for MLD. For VLANs, this allows you to configure MLD across more VLANs with fewer ports per VLAN, or fewer VLANs with more ports per VLAN. For LACPs, you can configure MLD across more LACP groups with fewer ports per LACP, or fewer LACP groups with more ports per LACP.

**Examples** To configure MLD Snooping on the VLAN interface `vlan2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping
```



To configure MLD Snooping on the VLAN interfaces v lan2 - v lan4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping
```

To disable MLD Snooping for the VLAN interface v lan2, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config)# no ipv6 mld snooping
```

To disable MLD Snooping for the VLAN interfaces v lan2 - v lan4, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config)# no ipv6 mld snooping
```

To configure MLD Snooping globally for the device, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 mld snooping
```

To disable MLD Snooping globally for the device, enter the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 mld snooping
```

## ipv6 mld snooping fast-leave

**Overview** Use this command to enable MLD Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing; the MLD group-membership is removed as soon as an MLD leave group message is received, without sending out a group-specific query.

Use the **no** variant of this command to disable fast-leave processing.

**Syntax** `ipv6 mld snooping fast-leave`  
`no ipv6 mld snooping fast-leave`

**Default** MLD Snooping fast-leave processing is disabled.

**Mode** Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

**Usage** This MLD Snooping command can only be configured on VLAN interfaces.

**Examples** This example shows how to enable fast-leave processing on the VLAN interface `vlan2`.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping fast-leave
```

This example shows how to enable fast-leave processing on the VLAN interface `vlan2- vlan4`.

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping fast-leave
```

# ipv6 mld snooping mrouter

**Overview** Use this command to statically configure the specified port as a Multicast Router interface for MLD Snooping within the specified VLAN.

See detailed usage notes below to configure static multicast router ports when using static IPv6 multicast routes with EPSR, and the destination VLAN is an EPSR data VLAN.

Use the **no** variant of this command to remove the static configuration of the interface as a Multicast Router interface.

**Syntax** `ipv6 mld snooping mrouter interface <port>`  
`no ipv6 mld snooping mrouter interface <port>`

| Parameter | Description                   |
|-----------|-------------------------------|
| <port>    | Specify the name of the port. |

**Mode** Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

**Usage** This MLD Snooping command statically configures a switch port as a Multicast Router interface.

Note that if static IPv6 multicast routing is being used with EPSR and the destination VLAN is an EPSR data VLAN, then multicast router (mrouter) ports must be statically configured. This minimizes disruption for multicast traffic in the event of ring failure or restoration.

When configuring the EPSR data VLAN, statically configure mrouter ports so that the multicast router can be reached in either direction around the EPSR ring.

For example, if port1.0.1 and port1.0.6 are ports on an EPSR data VLAN vlan101, which is the destination for a static IPv6 multicast route, then configure both ports as multicast router (mrouter) ports as shown in the example commands listed below:

**Output** Figure 21-1: Example **ipv6 mld snooping mrouter** commands when static IPv6 multicast routing is being used and the destination VLAN is an EPSR data VLAN:

```
awplus>enable
awplus#configure terminal
awplus(config)#interface vlan101
awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.1
awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.6
```

**Examples** This example shows how to specify the next-hop interface to the multicast router for VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping mrouter interface
port1.0.5
```

This example shows how to specify the next-hop interface to the multicast router for VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping mrouter interface
port1.0.5
```

**Related  
Commands** [ipv6 multicast route](#)

## ipv6 mld snooping querier

**Overview** Use this command to enable MLD querier operation on a subnet (VLAN) when no multicast routing protocol is configured in the subnet (VLAN). When enabled, the MLD Snooping querier sends out periodic MLD queries for all interfaces on that VLAN.

Use the **no** variant of this command to disable MLD querier configuration.

**Syntax** `ipv6 mld snooping querier`  
`no ipv6 mld snooping querier`

**Mode** Interface Configuration for a specified VLAN interface.

**Usage** This command can only be configured on a single VLAN interface - not on multiple VLANs.

The MLD Snooping querier uses the 0.0.0.0 Source IP address because it only masquerades as an MLD querier for faster network convergence.

The MLD Snooping querier does not start, or automatically cease, the MLD Querier operation if it detects query message(s) from a multicast router. It restarts as an MLD Snooping querier if no queries are seen within the other querier interval.

**Example** `awplus# configure terminal`  
`awplus(config)# interface vlan2`  
`awplus(config-if)# ipv6 mld snooping querier`

# ipv6 mld snooping report-suppression

**Overview** Use this command to enable report suppression from hosts for Multicast Listener Discovery version 1 (MLDv1) on a VLAN in Interface Configuration mode.

Use the **no** variant of this command to disable report suppression on a VLAN in Interface Configuration mode.

**Syntax** `ipv6 mld snooping report-suppression`  
`no ipv6 mld snooping report-suppression`

**Default** Report suppression does not apply to MLDv2, and is turned on by default for MLDv1 reports.

**Mode** Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

**Usage** This MLD Snooping command can only be configured on VLAN interfaces.

MLDv1 Snooping maybe configured to suppress reports from hosts. When a querier sends a query, only the first report for particular set of group(s) from a host will be forwarded to the querier by the MLD Snooping device. Similar reports (to the same set of groups) from other hosts, which would not change group memberships in the querier, will be suppressed by the MLD Snooping device to prevent 'flooding' of query responses.

**Examples** This example shows how to enable report suppression for MLD reports on VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping report-suppression
```

This example shows how to disable report suppression for MLD reports on VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 mld snooping report-suppression
```

This example shows how to enable report suppression for MLD reports on VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping report-suppression
```

This example shows how to disable report suppression for MLD reports on VLAN interfaces v l a n 2 - v l a n 4:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no ipv6 mld snooping report-suppression
```

## 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>|ssm-map] [interface <port>]`  
`no ipv6 mld static-group <ipv6-group-address> [source <ipv6-source-address>|ssm-map] [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>ssm-map</code>                     | Mode of defining SSM mapping. SSM mapping statically assigns sources to MLDv1 groups to translate these (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM.                                                                                            |
| <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 to that physical interface. If this parameter is not used, the static configuration is applied on all ports in the VLAN. |

**Mode** Interface Configuration for a VLAN interface.

**Usage** This command applies to MLD Snooping on a VLAN interface to statically add groups and/or source records.



**Examples** The following examples show how to statically add group and/or source records for MLD:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
fe80::2fd:6cff:fe1c:b
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
ssm-map
```

The following examples show how to statically add group and/or source records for MLD Snooping on VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
fe80::2fd:6cff:fe1c:b
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
ssm-map
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 interface
port1.0.4
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
fe80::2fd:6cff:fe1c:b interface port1.0.4
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
ssm-map interface port1.0.4
```

# show debugging mld

**Overview** Use this command to display the MLD debugging modes enabled with the [debug mld](#) command.

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 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 with receivers directly connected to the router, and learned through MLD.

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 ipv6 mld groups [<ipv6-address> |<interface>] [detail]

| Parameter      | Description                                                                  |
|----------------|------------------------------------------------------------------------------|
| <ipv6-address> | Optional. Specify Address of the multicast group in format X:X::X:X.         |
| <interface>    | Optional. Specify the Interface name for which to display local information. |

**Mode** User Exec and Privileged Exec

**Examples** The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups
```

## Output

|                                |         |           |          |         |                           |
|--------------------------------|---------|-----------|----------|---------|---------------------------|
| MLD Connected Group Membership |         |           |          |         |                           |
| Group                          | Address | Interface | Uptime   | Expires | Last Reporter             |
| ff08::1                        |         | port1.0.1 | 00:00:24 | stopped | fe80::eecd:6dff:fe6b:4783 |

The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups detail
```

## Output

|                                                               |                           |          |     |       |  |
|---------------------------------------------------------------|---------------------------|----------|-----|-------|--|
| MLD Connected Group Membership Details for port1.0.1          |                           |          |     |       |  |
| Interface:                                                    | port1.0.1                 |          |     |       |  |
| Group:                                                        | ff08::1                   |          |     |       |  |
| Uptime:                                                       | 00:00:13                  |          |     |       |  |
| Group mode:                                                   | Include ( )               |          |     |       |  |
| Last reporter:                                                | fe80::eecd:6dff:fe6b:4783 |          |     |       |  |
| Group source list: (R - Remote, M - SSM Mapping, S - Static ) |                           |          |     |       |  |
| Source Address                                                | Uptime                    | v2 Exp   | Fwd | Flags |  |
| 2001:db8:::1                                                  | 00:00:13                  | 00:04:07 | Yes | R     |  |
| 2002:db8:::3                                                  | 00:00:13                  | 00:04:07 | Yes | R     |  |

# 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show ipv6 mld interface [<interface>]

| Parameter   | Description     |
|-------------|-----------------|
| <interface> | Interface name. |

**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

```
awplus#show ipv6 mld interface

Interface vlan1 (Index 301)
 MLD Enabled, Active, Querier, Version 2 (default)
 Internet address is fe80::215:77ff:fec9:7468
 MLD interface has 0 group-record states
 MLD activity: 0 joins, 0 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 enabled on this interface
 MLD Snooping fast-leave is not enabled
 MLD Snooping querier is enabled
 MLD Snooping report suppression is enabled
```

# show ipv6 mld snooping mrrouter

**Overview** Use this command to display the multicast router interfaces, both configured and learned, in a VLAN. If you do not specify a VLAN interface then all the VLAN interfaces are displayed.

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 ipv6 mld snooping mrrouter [<interface>]

| Parameter   | Description                                                                                                                                |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <interface> | Optional. Specify the name of the VLAN interface. Note: If you do not specify a single VLAN interface, then all VLAN interfaces are shown. |

**Mode** User Exec and Privileged Exec

**Examples** The following command displays the multicast router interfaces in v lan2:

```
awplus# show ipv6 mld snooping mrrouter vlan2
```

## Output

```
awplus#show ipv6 mld snooping mrrouter vlan2
VLAN Interface Static/Dynamic
2 port1.0.2 Dynamically Learned
2 port1.0.3 Dynamically Learned
```

The following command displays the multicast router interfaces for all VLAN interfaces:

```
awplus# show ipv6 mld snooping mrrouter
```

## Output

```
awplus#show ipv6 mld snooping mrrouter
VLAN Interface Static/Dynamic
2 port1.0.2 Dynamically Learned
2 port1.0.3 Dynamically Learned
3 port1.0.4 Statically Assigned
3 port1.0.5 Statically Assigned
```

# show ipv6 mld snooping statistics

**Overview** Use this command to display MLD Snooping statistics data.

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 ipv6 mld snooping statistics interface <interface>

| Parameter   | Description                     |
|-------------|---------------------------------|
| <interface> | The name of the VLAN interface. |

**Mode** User Exec and Privileged Exec

**Example** The following command displays MLDv2 statistical information for vlan1:  
awplus# show ipv6 mld snooping statistics interface vlan1

## Output

```
awplus#show ipv6 mld snooping statistics interface vlan1
MLD Snooping statistics for vlan1
Interface: port1.0.1
Group: ff08::1
Uptime: 00:02:18
Group mode: Include ()
Last reporter: fe80::eecd:6dff:fe6b:4783
Group source list: (R - Remote, M - SSM Mapping, S - Static)
 Source Address Uptime v2 Exp Fwd Flags
 2001:db8::1 00:02:18 00:02:02 Yes R
 2001:db8::3 00:02:18 00:02:02 Yes R
```

# 22

## IPv4 Hardware Access Control List (ACL) Commands

### Introduction

**Overview** This chapter provides an alphabetical reference of IPv4 Hardware Access Control List (ACL) commands. It contains detailed command information and command examples about IPv4 hardware ACLs, which are applied directly to interfaces using the `access-group` command

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself.

- Text in parenthesis in command names indicates usage not keyword entry. For example, **access-list hardware (named)** indicates named IPv4 hardware ACLs entered as `access-list hardware <name>` where `<name>` is a placeholder not a keyword.
- Parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as **(access-list standard numbered filter)** represents command entry in the format shown in the syntax `[<sequence-number>] {deny|permit} {<source>|host <host-address>|any}`.
- Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Sub-modes** Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 22-1: IPv4 Hardware Access List Commands and Prompts

| Command Name                                       | Command Mode    | Prompt               |
|----------------------------------------------------|-----------------|----------------------|
| <code>show interface access-group</code>           | Privileged Exec | <code>awplus#</code> |
| <code>show access-list (IPv4 Hardware ACLs)</code> | Privileged Exec | <code>awplus#</code> |
| <code>show interface access-group</code>           | Privileged Exec | <code>awplus#</code> |

Table 22-1: IPv4 Hardware Access List Commands and Prompts (cont.)

| Command Name                              | Command Mode                    | Prompt                    |
|-------------------------------------------|---------------------------------|---------------------------|
| access-group                              | Global Configuration            | awplus(config)#           |
| access-list (hardware IP numbered)        | Global Configuration            | awplus(config)#           |
| access-list (hardware MAC numbered)       | Global Configuration            | awplus(config)#           |
| access-list hardware (named)              | Global Configuration            | awplus(config)#           |
| access-group                              | Interface Configuration         | awplus(config-if)#        |
| (access-list hardware ICMP filter)        | IPv4 Hardware ACL Configuration | awplus(config-ip-hw-acl)# |
| (access-list hardware IP protocol filter) | IPv4 Hardware ACL Configuration | awplus(config-ip-hw-acl)# |
| (access-list hardware MAC filter)         | IPv4 Hardware ACL Configuration | awplus(config-ip-hw-acl)# |
| (access-list hardware TCP UDP filter)     | IPv4 Hardware ACL Configuration | awplus(config-ip-hw-acl)# |
| commit (IPv4)                             | IPv4 Hardware ACL Configuration | awplus(config-ip-hw-acl)# |

**References** For descriptions of ACLs, and further information about rules when applying them, see the [ACL Feature Overview and Configuration Guide](#).

For more information on link aggregation see the following references:

- the [Link Aggregation Feature Overview and Configuration Guide](#).
- [Link Aggregation Commands](#)

- Command List**
- “access-group” on page 681
  - “access-list (hardware IP numbered)” on page 683
  - “access-list (hardware MAC numbered)” on page 691
  - “access-list hardware (named)” on page 693
  - “(access-list hardware ICMP filter)” on page 695
  - “(access-list hardware IP protocol filter)” on page 698
  - “(access-list hardware MAC filter)” on page 704
  - “(access-list hardware TCP UDP filter)” on page 707
  - “commit (IPv4)” on page 710
  - “show access-list (IPv4 Hardware ACLs)” on page 711
  - “show interface access-group” on page 713



## access-group

**Overview** This command adds or removes a hardware-based access-list to or from a switch port interface. The number of hardware numbered and named access-lists that can be added to a switch port interface is determined by the available memory in hardware-based packet classification tables.

This command works in Interface Configuration mode to apply hardware access-lists to selected switch port interfaces.

The **no** variant of this command removes the selected access-list from an interface.

**Syntax** access-group  
[<3000-3699> | <4000-4699> | <hardware-access-list-name>]  
no access-group  
[<3000-3699> | 4000-4699 | <hardware-access-list-name>]

| Parameter                   | Description                    |
|-----------------------------|--------------------------------|
| <3000-3699>                 | Hardware IP access-list.       |
| <4000-4699>                 | Hardware MAC access-list.      |
| <hardware-access-list-name> | The hardware access-list name. |

**Mode** Interface Configuration for a switch port interface

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage** First create an IP access-list that applies the appropriate permit/deny requirements with the [access-list \(hardware IP numbered\)](#) command, the [access-list \(hardware MAC numbered\)](#) command or the [access-list hardware \(named\)](#) command. Then use this command to apply this hardware access-list to a specific port or port range. Note that this command will apply the access-list only to incoming data packets.

To apply ACLs to an LACP aggregated link, apply it to all the individual switch ports in the aggregated group. To apply ACLs to a static channel group, apply it to the static channel group itself. An ACL can even be applied to a static aggregated link that spans more than one switch instance ([Link Aggregation Commands](#)).

Note that you cannot apply software numbered ACLs to switch port interfaces with the access-group command. This command will only apply hardware ACLs.

**NOTE:** Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples** To add the numbered hardware access-list 3005 to switch port interface port1.0.1, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# access-group 3005
```

To add the named hardware access-list `hw-acl` to switch port interface `port1.0.2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# access-group hw-acl
```

To apply an ACL to static channel group 2 containing switch `port1.0.5` and `port1.0.6`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5-1.0.6
awplus(config-if)# static-channel-group 2
awplus(config)# interface sa2
awplus(config-if)# access-group 3000
```

**Related  
Commands**

[access-list hardware \(named\)](#)  
[access-list \(hardware IP numbered\)](#)  
[access-list \(hardware MAC numbered\)](#)  
[show interface access-group](#)

## access-list (hardware IP numbered)

**Overview** This command creates an access-list for use with hardware classification, such as QoS. The access-list will match on either TCP or UDP type packets that have the specified source and destination IP addresses and Layer 4 port values or ranges. The parameter **any** may be specified if an address does not matter and the port values are optional.

The **no** variant of this command removes the previously specified IP hardware access-list.

**Syntax [ip]** access-list <3000-3699> {deny|permit|send-to-cpu} ip <source> <destination>

**Syntax [icmp]** access-list <3000-3699> {deny|permit|send-to-cpu} icmp <source> <destination> [icmp-type <type-number>]

no access-list <3000-3699>

Table 22-2: **Parameters in the access-list (hardware IP numbered) command - ip|icmp**

| Parameter   | Description                                                                                                                                                                      |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <3000-3699> | Hardware IP access-list number.                                                                                                                                                  |
| deny        | Access-list rejects packets that match the source and destination filtering specified with this command.                                                                         |
| permit      | Access-list permits packets that match the source and destination filtering specified with this command.                                                                         |
| send-to-cpu | Specify packets to send to the CPU.                                                                                                                                              |
| icmp        | ICMP packet.                                                                                                                                                                     |
| ip          | IP packet.                                                                                                                                                                       |
| <source>    | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                       |
|             | any Matches any source IP address.                                                                                                                                               |
|             | host<ip-addr> Matches a single source host with the IP address given by <ip-addr> in dotted decimal notation.                                                                    |
|             | <ip-addr>/<prefix> An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.                         |
|             | <ip-addr><reverse-mask> Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.10.0.0.255 is the same as entering 192.168.1.1/24. |

Table 22-2: **Parameters in the access-list (hardware IP numbered) command - ip|icmp (cont.)**

| Parameter                   | Description                                                                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;destination&gt;</i>  | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:   |
| any                         | Matches any destination IP address.                                                                                                                                         |
| host<ip-addr>               | Matches a single destination host with the IP address given by <ip-addr> in dotted decimal notation.                                                                        |
| <ip-addr>/<br><prefix>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                  |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1/24. |
| icmp-type                   | Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.                                                         |
| <type-number>               | The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:                                         |
| 0                           | Echo replies.                                                                                                                                                               |
| 3                           | Destination unreachable messages.                                                                                                                                           |
| 4                           | Source quench messages.                                                                                                                                                     |
| 5                           | Redirect (change route) messages.                                                                                                                                           |
| 8                           | Echo requests.                                                                                                                                                              |
| 11                          | Time exceeded messages.                                                                                                                                                     |
| 12                          | Parameter problem messages.                                                                                                                                                 |
| 13                          | Timestamp requests.                                                                                                                                                         |
| 14                          | Timestamp replies.                                                                                                                                                          |
| 15                          | Information requests.                                                                                                                                                       |
| 16                          | Information replies.                                                                                                                                                        |
| 17                          | Address mask requests.                                                                                                                                                      |
| 18                          | Address mask replies.                                                                                                                                                       |

**Syntax [tcp|udp]** access-list <3000-3699> {deny|permit|send-to-cpu} {tcp|udp} <source> eq <sourceport> <destination> eq <destport>  
no access-list <3000-3699>

Table 22-3: **Parameters in the access-list (hardware IP numbered) command - tcp|udp**

| Parameter   | Description                                                                                                                                                                           |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <3000-3699> | Hardware IP access-list.                                                                                                                                                              |
| deny        | The access-list rejects packets that match the type, source, and destination filtering specified with this command.                                                                   |
| permit      | The access-list permits packets that match the type, source, and destination filtering specified with this command.                                                                   |
| send-to-cpu | Specify packets to send to the CPU.                                                                                                                                                   |
| tcp         | The access-list matches only TCP packets.                                                                                                                                             |
| udp         | The access-list matches only UDP packets.                                                                                                                                             |
| <source>    | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                            |
|             | any Matches any source IP address.                                                                                                                                                    |
|             | host<ip-addr> Matches a single source host with the IP address given by <ip-addr> in dotted decimal notation.                                                                         |
|             | <ip-addr>/<prefix> An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.                              |
|             | <ip-addr><br><reverse-mask> Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24. |

Table 22-3: **Parameters in the access-list (hardware IP numbered) command - tcp|udp (cont.)**

| Parameter                   | Description                                                                                                                                                               |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;destination&gt;</i>  | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination: |
| any                         | Matches any destination IP address.                                                                                                                                       |
| host<ip-addr>               | Matches a single destination host with the IP address given by <ip-addr> in dotted decimal notation.                                                                      |
| <ip-addr>/<prefix>          | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.                 |
| <sourceport>                | The source (TCP or UDP) port number, specified as an integer between 0 and 65535.                                                                                         |
| eq                          | Matches port numbers that are equal to the port number specified immediately after this parameter.                                                                        |

**Syntax [proto]** access-list <3000-3699> {deny|permit|send-to-cpu} proto  
<ip-protocol> <source> <destination>  
no access-list <3000-3699>

Table 22-4: **Parameters in the access-list (hardware IP numbered) command - proto**

| Parameter   | Description                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------|
| <3000-3699> | Hardware IP access-list.                                                                                 |
| deny        | Access-list rejects packets that match the source and destination filtering specified with this command. |
| permit      | Access-list permits packets that match the source and destination filtering specified with this command. |
| send-to-cpu | Specify packets to send to the CPU.                                                                      |

Table 22-4: **Parameters in the access-list (hardware IP numbered) command - proto (cont.)**

| Parameter                   | Description                                                                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;source&gt;</b>       | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                  |
| any                         | Matches any source IP address.                                                                                                                                              |
| host<ip-addr>               | Matches a single source host with the IP address given by <ip-addr> in dotted decimal notation.                                                                             |
| <ip-addr>/<br><prefix>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.                                       |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1/24. |
| <b>&lt;destination&gt;</b>  | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:   |
| any                         | Matches any destination IP address.                                                                                                                                         |
| host<ip-addr>               | Matches a single destination host with the IP address given by <ip-addr> in dotted decimal notation.                                                                        |
| <ip-addr>/<br><prefix>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                  |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1/24. |
| proto                       | Matches only a specified type of IP Protocol <1-255>.                                                                                                                       |

Table 22-4: **Parameters in the access-list (hardware IP numbered) command - proto (cont.)**

| Parameter     | Description                                                                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-protocol> | The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority)<br><a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a> |
|               | Protocol Number      Protocol Description [RFC Reference]                                                                                                                                    |
|               | 1      Internet Control Message [RFC792]                                                                                                                                                     |
|               | 2      Internet Group Management [RFC1112]                                                                                                                                                   |
|               | 3      Gateway-to-Gateway [RFC823]                                                                                                                                                           |
|               | 4      IP in IP [RFC2003]                                                                                                                                                                    |
|               | 5      Stream [RFC1190] [RFC1819]                                                                                                                                                            |
|               | 6      TCP (Transmission Control Protocol) [RFC793]                                                                                                                                          |
|               | 8      EGP (Exterior Gateway Protocol) [RFC888]                                                                                                                                              |
|               | 9      IGP (Interior Gateway Protocol) [IANA]                                                                                                                                                |
|               | 11      Network Voice Protocol [RFC741]                                                                                                                                                      |
|               | 17      UDP (User Datagram Protocol) [RFC768]                                                                                                                                                |
|               | 20      Host monitoring [RFC869]                                                                                                                                                             |
|               | 27      RDP (Reliable Data Protocol) [RFC908]                                                                                                                                                |
|               | 28      IRTP (Internet Reliable Transaction Protocol) [RFC938]                                                                                                                               |
|               | 29      ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]                                                                                                                                    |



Table 22-4: **Parameters in the access-list (hardware IP numbered) command - proto (cont.)**

| Parameter            | Description                                              |
|----------------------|----------------------------------------------------------|
| <ip-protocol>(cont.) | 30 Bulk Data Transfer Protocol [RFC969]                  |
|                      | 33 DCCP (Datagram Congestion Control Protocol) [RFC4340] |
|                      | 48 DSR (Dynamic Source Routing Protocol) [RFC4728]       |
|                      | 50 ESP (Encap Security Payload) [RFC2406]                |
|                      | 51 AH (Authentication Header) [RFC2402]                  |
|                      | 54 NARP (NBMA Address Resolution Protocol) [RFC1735]     |
|                      | 88 EIGRP (Enhanced Interior Gateway Routing Protocol)    |
|                      | 89 OSPFIGP [RFC1583]                                     |
|                      | 97 Ethernet-within-IP Encapsulation / RFC3378            |
|                      | 98 Encapsulation Header / RFC1241                        |
|                      | 108 IP Payload Compression Protocol / RFC2393            |
|                      | 112 Virtual Router Redundancy Protocol / RFC3768         |
|                      | 134 RSVP-E2E-IGNORE / RFC3175                            |
|                      | 135 Mobility Header / RFC3775                            |
|                      | 136 UDPLite / RFC3828                                    |
|                      | 137 MPLS-in-IP / RFC4023                                 |
|                      | 138 MANET Protocols / RFC-ietf-manet-iana-07.txt         |
|                      | 139-252 Unassigned / IANA                                |
|                      | 253 Use for experimentation and testing / RFC3692        |
|                      | 254 Use for experimentation and testing / RFC3692        |
|                      | 255 Reserved / IANA                                      |

**Mode** Global Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage** This command creates an access-list for use with hardware classification, such as when applying QoS. This command can be used to match ICMP packets, IP protocols, or TCP/ UDP packets.

For ICMP packets, the <3000-3699> range IP hardware access-list will match any ICMP packet that has the specified source and destination IP addresses and ICMP type.

You may apply the **any** parameter if the source or destination IP address is not important. The ICMP type is an optional parameter.

**NOTE:** Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples** Follow the below example commands to configure access-lists for ICMP, IP protocol and TCP.

**ICMP Example** To create an access-list that will permit ICMP packets with a source address of 192.168.1.0/24 with any destination address and an ICMP type of 5 enter the below commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit icmp 192.168.1.0/24 any
icmp-type 5
```

To destroy the access-list with an access-list identity of 3000 enter the below commands:

```
awplus# configure terminal
awplus(config)# no access-list 3000
```

**IP Example** To create an access-list that will permit any type of IP packet with a source address of 192.168.1.1 and any destination address, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit ip 192.168.1.1/32 any
```

To create an access-list that will deny all IGMP packets (IP protocol 2) from the 192.168.0.0 network, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 deny proto 2 192.168.0.0/16
any
```

**TCP Example** To create an access-list that will permit TCP packets with a destination address of 192.168.1.1, a destination port of 80 and any source address and source port, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit tcp any 192.168.1.1/32
eq 80
```

**Related  
Commands**

- [access-group](#)
- [mirror interface](#)
- [show running-config](#)
- [show access-list \(IPv4 Hardware ACLs\)](#)

## access-list (hardware MAC numbered)

**Overview** This command creates an access-list for use with hardware classification, such as QoS. The access-list will match on packets that have the specified source and destination MAC addresses. The parameter **any** may be specified if an address does not matter.

The **no** variant of this command removes the specified MAC hardware filter access-list.

**Syntax** `access-list <4000-4699> {deny|permit|send-to-cpu}  
{<source-mac-address>  
<source-mac-mask>|any}{<destination-mac-address>  
<destination-mac-mask>|any}  
no access-list <4000-4699>`

| Parameter                 | Description                                                                                                                                                                                                                                                                                 |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <4000-4699>               | Hardware MAC access-list.                                                                                                                                                                                                                                                                   |
| deny                      | Access-list rejects packets that match the source and destination filtering.                                                                                                                                                                                                                |
| permit                    | Access-list permits packets that match the source and destination filtering.                                                                                                                                                                                                                |
| send-to-cpu               | Specify packets to send to the CPU.                                                                                                                                                                                                                                                         |
| <source-mac-address>      | The source MAC address of the packets.<br>Enter this in the format <HHHH.HHHH.HHHH><br>where each <i>H</i> is a hexadecimal number that represents a 4 bit binary number.                                                                                                                   |
| <source-mac-mask          | The mask that will be applied to the source MAC addresses.<br>Enter this in the format <HHHH.HHHH.HHHH><br>where each <i>H</i> is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either 0 or F. Where Hex FF = Ignore, and Hex 00 = Match.      |
| any                       | Any source MAC address.                                                                                                                                                                                                                                                                     |
| <destination-mac-address> | The destination MAC address of the packets.<br>Enter this in the format <HHHH.HHHH.HHHH><br>where each <i>H</i> is a hexadecimal number that represents a 4 bit binary number.                                                                                                              |
| <destination-mac-mask>    | The mask that will be applied to the destination MAC addresses.<br>Enter this in the format <HHHH.HHHH.HHHH><br>where each <i>H</i> is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either 0 or F. Where Hex FF = Ignore, and Hex 00 = Match. |
| any                       | Any destination MAC address.                                                                                                                                                                                                                                                                |

| Parameter  | Description                                                                                                                                                                                                       |
|------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| vlan       | Specifies that the ACL will match on the ID in the packet's VLAN tag.                                                                                                                                             |
| <1 - 4094> | The VLAN VID.                                                                                                                                                                                                     |
| inner-vlan | This parameter is used within double-tagged VLANs. It is the inner VLAN tag (VID); sometimes referred to as the C-TAG (Customer VLAN TAG), where the vlan VID tag is referred to as the S-TAG (Service VLAN TAG). |
| <1 - 4094> | The inner VLAN VID.                                                                                                                                                                                               |

**Mode** Global Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage** This command creates an access-list for use with hardware classification, such as when applying QoS. The <4000-4699> range MAC hardware access-list will match on packets that have the specified source and destination MAC addresses. You may apply the **any** parameter if the source or destination MAC host address is not important.

**NOTE:** Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples** To create an access-list that will permit packets with a MAC address of 0000.00ab.1234 and any destination address enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 4000 permit 0000.00ab.1234
0000.0000.0000 any
```

To create an access-list that will permit packets with an initial MAC address component of 0000.00ab and any destination address, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 permit 0000.00ab.1234
0000.0000.FFFF any
```

To destroy the access-list with an access-list identity of 4000 enter the commands:

```
awplus# configure terminal
awplus(config)# no access-list 4000
```

**Related Commands**

- [access-group](#)
- [mirror interface](#)
- [show running-config](#)
- [show access-list \(IPv4 Hardware ACLs\)](#)

## access-list hardware (named)

**Overview** This command creates a named hardware access-list that can be applied to a switch port interface. ACL filters for a named hardware ACL are created in the IPv4 Hardware ACL Configuration mode.

The **no** variant of this command removes the specified named hardware ACL.

**Syntax** `access-list hardware <hardware-access-list-name>`  
`no access-list hardware <hardware-access-list-name>`

| Parameter                                      | Description                                                                                                          |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <code>&lt;hardware-access-list-name&gt;</code> | Specify the hardware ACL name to then define ACL filters for in the subsequent IPv4 Hardware ACL Configuration mode. |

**Mode** Global Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage** Use this command to name a hardware ACL and enter the IPv4 Hardware ACL Configuration mode. If the named hardware ACL doesn't exist, it will be created after entry. If the named hardware ACL does exist, then you can enter IPv4 Hardware ACL Configuration mode for that existing ACL.

Entering this command with the hardware ACL name moves you to the (config-ip-hw-acl) prompt for the IPv4 Hardware ACL Configuration mode so you can enter ACL filters with sequence numbers. From this prompt, configure the filters for the ACL. See the [ACL Feature Overview and Configuration Guide](#) for complete examples of configured sequenced numbered ACLs.

**NOTE:** Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples** To create the hardware access-list named ACL - 1 and enter the IPv4 Hardware ACL Configuration mode to specify the ACL filter entry, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware ACL-1
awplus(config-ip-hw-acl)#
```

To remove the hardware access-list named ACL - 1, use the commands:

```
awplus# configure terminal
awplus(config)# no access-list hardware ACL-1
```

**Related  
Commands**

- [access-group](#)
- [\(access-list hardware ICMP filter\)](#)
- [\(access-list hardware IP protocol filter\)](#)
- [\(access-list hardware TCP UDP filter\)](#)
- [\(access-list standard named filter\)](#)
- [show access-list \(IPv4 Hardware ACLs\)](#)

## (access-list hardware ICMP filter)

**Overview** Use this ACL filter to add a new ICMP filter entry to the current hardware access-list. The filter will match on any ICMP packet that has the specified source and destination IP addresses and ICMP type. The parameter **any** may be specified if an address does not matter and the ICMP type is an optional parameter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an ICMP filter entry from the current hardware access-list. You can specify the ICMP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its ICMP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the command, the [show access-list \(IPv4 Hardware ACLs\)](#) command.

**Syntax [icmp]** [*<sequence-number>*] {deny|permit|send-to-cpu} icmp *<source>* *<destination>* [icmp *<icmp-value>*]  
no {deny|permit|send-to-cpu} icmp *<source>* *<destination>* [icmp *<icmp-value>*]  
no *<sequence-number>*

| Parameter                      | Description                                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------------------|
| <i>&lt;sequence-number&gt;</i> | <1-65535><br>The sequence number for the filter entry of the selected access control list.               |
| deny                           | Access-list rejects packets that match the source and destination filtering specified with this command. |
| permit                         | Access-list permits packets that match the source and destination filtering specified with this command. |
| send-to-cpu                    | Specify packets to send to the CPU.                                                                      |
| icmp                           | ICMP packet type.                                                                                        |

| Parameter                                             | Description                                                                                                                                                                 |
|-------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;source&gt;</code>                           | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                  |
| <code>&lt;ip-addr&gt;/<br/>&lt;prefix&gt;</code>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.                                       |
| <code>&lt;ip-addr&gt;<br/>&lt;reverse-mask&gt;</code> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1/24. |
| <code>host&lt;ip-addr&gt;</code>                      | Matches a single source host with the IP address given by <code>&lt;ip-addr&gt;</code> in dotted decimal notation.                                                          |
| <code>any</code>                                      | Matches any source IP address.                                                                                                                                              |
| <code>&lt;destination&gt;</code>                      | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:   |
| <code>&lt;ip-addr&gt;/<br/>&lt;prefix&gt;</code>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                  |
| <code>&lt;ip-addr&gt;<br/>&lt;reverse-mask&gt;</code> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1/24. |
| <code>host&lt;ip-addr&gt;</code>                      | Matches a single destination host with the IP address given by <code>&lt;ip-addr&gt;</code> in dotted decimal notation.                                                     |
| <code>any</code>                                      | Matches any destination IP address.                                                                                                                                         |
| <code>icmp-type</code>                                | The ICMP type.                                                                                                                                                              |
| <code>&lt;icmp-value&gt;</code>                       | The value of the ICMP type.                                                                                                                                                 |

**Mode** IPv4 Hardware ACL Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage** First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the [access-group](#) command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.



An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** You must reach the prompt `awplus(config-ip-hw-acl)#` by running the `access-list hardware (named)` command, and entering an appropriate access-list name.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples** To add an access-list filter entry with a sequence number of 100 to the access-list named `my-list` that will permit ICMP packets with a source address of `192.168.1.0/24`, any destination address and an icmp type of 5, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# 100 permit icmp 192.168.1.0/24 any
icmp-type 5
```

To remove an access-list filter entry with a sequence number of 100 in the access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# no 100
```

**Related Commands**

- `access-list hardware (named)`
- `show running-config`
- `show access-list (IPv4 Hardware ACLs)`

## (access-list hardware IP protocol filter)

**Overview** Use this ACL filter to add an IP protocol type filter entry to the current hardware access-list. The filter will match on any IP packet that has the specified source and destination IP addresses and IP protocol type, or has the optionally specified source and destination MAC addresses. The parameter **any** may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP protocol type filter entry from the current hardware access-list. You can specify the IP protocol type filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP protocol type filter profile without specifying its sequence number.

Note that the sequence number can be found by running the [show access-list \(IPv4 Hardware ACLs\)](#) command.

**Syntax** [**any|ip|proto**] [`<sequence-number>`] {deny|permit|send-to-cpu} {any|ip|proto `<ip-protocol>`} {`<source>`|dhcp snooping|any} {`<destination>`|any} [mac {`<mac-source-address>` `<mac-source-mask>`|any} {`<mac-destination-address>` `<mac-destination-mask>`|any}]

no {deny|permit|send-to-cpu} {any|ip|proto `<ip-protocol>`} {`<source>`|dhcp snooping} {`<destination>`|any} [mac {`<mac-source-address>` `<mac-source-mask>`|any} {`<mac-destination-address>` `<mac-destination-mask>`|any}]

no `<sequence-number>`

| Parameter                              | Description                                                                                                     |
|----------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| <code>&lt;sequence-number&gt;</code>   | <code>&lt;1 - 65535&gt;</code><br>The sequence number for the filter entry of the selected access control list. |
| deny                                   | Access-list rejects packets of the type specified.                                                              |
| permit                                 | Access-list allows packets of the type specified                                                                |
| send to cpu                            | Specify packets to send to the CPU.                                                                             |
| ip                                     | IP packets.                                                                                                     |
| any                                    | Any packet.                                                                                                     |
| proto <code>&lt;ip-protocol&gt;</code> | The IP Protocol type specified by it protocol number <code>&lt;1-255&gt;</code> .                               |

| Parameter     | Description                                                                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-protocol> | The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority)<br><a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a> |
|               | Protocol Number      Protocol Description [RFC Reference]                                                                                                                                    |
|               | 1      Internet Control Message [RFC792]                                                                                                                                                     |
|               | 2      Internet Group Management [RFC1112]                                                                                                                                                   |
|               | 3      Gateway-to-Gateway [RFC823]                                                                                                                                                           |
|               | 4      IP in IP [RFC2003]                                                                                                                                                                    |
|               | 5      Stream [RFC1190] [RFC1819]                                                                                                                                                            |
|               | 6      TCP (Transmission Control Protocol) [RFC793]                                                                                                                                          |
|               | 8      EGP (Exterior Gateway Protocol) [RFC888]                                                                                                                                              |
|               | 9      IGP (Interior Gateway Protocol) [IANA]                                                                                                                                                |
|               | 11      Network Voice Protocol [RFC741]                                                                                                                                                      |
|               | 17      UDP (User Datagram Protocol) [RFC768]                                                                                                                                                |
|               | 20      Host monitoring [RFC869]                                                                                                                                                             |
|               | 27      RDP (Reliable Data Protocol) [RFC908]                                                                                                                                                |
|               | 28      IRTP (Internet Reliable Transaction Protocol) [RFC938]                                                                                                                               |
|               | 29      ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]                                                                                                                                    |
|               | 30      Bulk Data Transfer Protocol [RFC969]                                                                                                                                                 |
|               | 33      DCCP (Datagram Congestion Control Protocol) [RFC4340]                                                                                                                                |
|               | 48      DSR (Dynamic Source Routing Protocol) [RFC4728]                                                                                                                                      |
|               | 50      ESP (Encap Security Payload) [RFC2406]                                                                                                                                               |
|               | 51      AH (Authentication Header) [RFC2402]                                                                                                                                                 |

| Parameter            | Description                                                         |                                                    |
|----------------------|---------------------------------------------------------------------|----------------------------------------------------|
| <ip-protocol>(cont.) | 54                                                                  | NARP (NBMA Address Resolution Protocol) [RFC1735]  |
|                      | 58                                                                  | ICMP for IPv6 [RFC1883]                            |
|                      | 59                                                                  | No Next Header for IPv6 [RFC1883]                  |
|                      | 60                                                                  | Destination Options for IPv6 [RFC1883]             |
|                      | 88                                                                  | EIGRP (Enhanced Interior Gateway Routing Protocol) |
|                      | 89                                                                  | OSPFv2 [RFC1583]                                   |
|                      | 97                                                                  | Ethernet-within-IP Encapsulation / RFC3378         |
|                      | 98                                                                  | Encapsulation Header / RFC1241                     |
|                      | 108                                                                 | IP Payload Compression Protocol / RFC2393          |
|                      | 112                                                                 | Virtual Router Redundancy Protocol / RFC3768       |
|                      | 134                                                                 | RSVP-E2E-IGNORE / RFC3175                          |
|                      | 135                                                                 | Mobility Header / RFC3775                          |
|                      | 136                                                                 | UDPLite / RFC3828                                  |
|                      | 137                                                                 | MPLS-in-IP / RFC4023                               |
|                      | 138                                                                 | MANET Protocols / RFC-ietf-manet-iana-07.txt       |
|                      | 139-252                                                             | Unassigned / IANA                                  |
|                      | 253                                                                 | Use for experimentation and testing / RFC3692      |
|                      | 254                                                                 | Use for experimentation and testing / RFC3692      |
|                      | 255                                                                 | Reserved / IANA                                    |
| dhcpsnooping         | The source address learned from the DHCP Snooping binding database. |                                                    |

| Parameter                  | Description                                                                                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;source&gt;</b>      | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                |
| any                        | Matches any source IP address.                                                                                                                                            |
| host<ip-addr>              | Matches a single source host with the IP address given by <ip-addr> in dotted decimal notation.                                                                           |
| <ip-addr>/<prefix>         | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.                                     |
| <ip-addr><reverse-mask>    | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.                 |
| <b>&lt;destination&gt;</b> | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination: |
| any                        | Matches any destination IP address.                                                                                                                                       |
| host<ip-addr>              | Matches a single destination host with the IP address given by <ip-addr> in dotted decimal notation.                                                                      |
| <ip-addr>/<prefix>         | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                |
| <ip-addr><reverse-mask>    | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.                 |
| mac                        | Signifies a MAC and based hardware access-list.                                                                                                                           |
| <mac-source-address>       | The source host's MAC address, entered in HHHH.HHHH.HHHH format.                                                                                                          |
| <mac-source-mask>          | The source host's MAC wildcard mask entered in HHHH.HHHH.HHHH format.<br>where Hex FF = Ignore, and Hex 00 = Match.                                                       |
| any                        | Matches any source MAC address.                                                                                                                                           |

| Parameter                 | Description                                                                                                          |
|---------------------------|----------------------------------------------------------------------------------------------------------------------|
| <mac-destination-address> | The destination host's MAC address, entered in HHHH.HHHH.HHHH format.                                                |
| <mac-destination-mask>    | The destination host's wildcard mask entered in HHHH.HHHH.HHHH format.<br>where Hex FF = Ignore, and Hex 00 = Match. |
| any                       | Matches any destination MAC address.                                                                                 |

**Mode** IPv4 Hardware ACL Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage** First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the [access-group](#) command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the [access-list hardware \(named\)](#) command. with the required access control list number, or name, but with no further parameters selected.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples** To add an access-list filter entry to the access-list named my - list that will permit any type of IP packet with a source address of 192 . 168 . 1 . 1 and any destination address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit ip 192.168.1.1/32 any
```

To add an access-list filter entry to the access-list named my - list that will permit any type of IP packet with a source address of 192 . 168 . 1 . 1 and a MAC source address of ffee . ddcc . bbaa with any IP and MAC destination address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit ip 192.168.1.1/32 any mac
ffee.ddcc.bbaa any
```

To add an access-list filter entry to the access-list named my-list a filter that will deny all IGMP packets (protocol 2) from the 192.168.0.0 network with sequence number 50 in access-list, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# 50 deny proto 2 192.168.0.0/16 any
```

**Related  
Commands**

[access-list hardware \(named\)](#)  
[show running-config](#)  
[show access-list \(IPv4 Hardware ACLs\)](#)

## (access-list hardware MAC filter)

**Overview** Use this ACL filter to add a MAC filter entry to the current hardware access-list. The filter will match on any IP packet that has the specified source and destination MAC addresses. The parameter **any** may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a MAC filter entry from the current hardware access-list. You can specify the MAC filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its MAC filter profile without specifying its sequence number.

Note that the sequence number can be found by running the [show access-list \(IPv4 Hardware ACLs\)](#) command.

**Syntax [mac]** [*<sequence-number>*] {deny|permit|send-to-cpu} mac {*<source-mac-address>* *<source-mac-mask>*|any} {*<destination-mac-address>* *<destination-mac-mask>*|any}  
no {deny|permit|send-to-cpu} mac {*<source-mac-address>* *<source-mac-mask>*|any} {*<destination-mac-address>* *<destination-mac-mask>*|any}  
no *<sequence-number>*

| Parameter                         | Description                                                                                                                                                                                                                                                                     |
|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;sequence-number&gt;</i>    | <1 - 65535><br>The sequence number for the filter entry of the selected access control list.                                                                                                                                                                                    |
| deny                              | Specify packets to reject.                                                                                                                                                                                                                                                      |
| permit                            | Specify packets to accept.                                                                                                                                                                                                                                                      |
| send-to-cpu                       | Specify packets to send to the CPU.                                                                                                                                                                                                                                             |
| mac                               | MAC address.                                                                                                                                                                                                                                                                    |
| <i>&lt;source-mac-address&gt;</i> | The source MAC address of the packets.<br>Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number.                                                                                                                 |
| <i>&lt;source-mac-mask&gt;</i>    | The mask that will be applied to the source MAC addresses.<br>Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either 0 or F.<br>Where Hex FF = Ignore, and Hex 00 = Match. |
| any                               | Any source MAC host.                                                                                                                                                                                                                                                            |



| Parameter                                    | Description                                                                                                                                                                                                                                                                                       |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;destination-mac-address&gt;</code> | The destination MAC address of the packets. Enter this in the format <code>&lt;HHHH.HHHH.HHHH&gt;</code> where each H is a hexadecimal number that represents a 4 bit binary number.                                                                                                              |
| <code>&lt;destination-mac-mask&gt;</code>    | The mask that will be applied to the destination MAC addresses. Enter this in the format <code>&lt;HHHH.HHHH.HHHH&gt;</code> where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either 0 or F. Where Hex FF = Ignore, and Hex 00 = Match. |
| any                                          | Any destination MAC host.                                                                                                                                                                                                                                                                         |

**Mode** IPv4 Hardware ACL Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage** First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the [access-group](#) command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number

**NOTE:** The access control list being configured is selected by running the [access-list hardware \(named\)](#) command. with the required access control list number, or name, but with no further parameters selected.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples** To add an access-list filter entry to the access-list named my-list that will permit packets with a source MAC address of 0000.00ab.1234 and any destination MAC address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit mac 0000.00ab.1234
0000.0000.0000 any
```

To remove an access-list filter entry that permit packets with a source MAC address of 0000.00ab.1234 and any destination MAC address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# no permit mac 0000.00ab.1234
0000.0000.0000 any
```

**Related  
Commands**    [access-group](#)  
                  [access-list hardware \(named\)](#)  
                  [show running-config](#)

## (access-list hardware TCP UDP filter)

**Overview** Use this ACL filter to add a TCP or UDP filter entry to the current hardware access-list. The filter will match on any TCP or UDP type packet that has the specified source and destination IP addresses. The parameter **any** may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a TCP or UDP filter entry from the current hardware access-list. You can specify the TCP or UDP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its TCP or UDP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the [show access-list \(IPv4 Hardware ACLs\)](#) command.

**Syntax [tcp|udp]** [*<sequence-number>*] {deny|permit|send-to-cpu} {tcp|udp}  
<source> eq <sourceport> <destination> eq <destport>  
no {deny|permit|send-to-cpu} {tcp|udp} <source> eq <sourceport>  
<destination>eq <destport>  
no <sequence-number>

| Parameter         | Description                                                                                              |
|-------------------|----------------------------------------------------------------------------------------------------------|
| <sequence-number> | <1 - 65535><br>The sequence number for the filter entry of the selected access control list.             |
| deny              | Access-list rejects packets that match the source and destination filtering specified with this command. |
| permit            | Access-list permits packets that match the source and destination filtering specified with this command. |
| send-to-cpu       | Specify packets to send to the CPU.                                                                      |
| tcp               | TCP packets.                                                                                             |
| udp               | UDP packets.                                                                                             |

| Parameter                   | Description                                                                                                                                                               |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;source&gt;</b>       | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                |
| any                         | Matches any source IP address.                                                                                                                                            |
| host<ip-addr>               | Matches a single source host with the IP address given by <ip-addr> in dotted decimal notation.                                                                           |
| <ip-addr>/<br><prefix>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.                                     |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.                 |
| <b>&lt;sourceport&gt;</b>   | The source TCP or UDP port number, specified as an integer between 0 and 65535.                                                                                           |
| <b>&lt;destination&gt;</b>  | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination: |
| any                         | Matches any destination IP address.                                                                                                                                       |
| host<ip-addr>               | Matches a single destination host with the IP address given by <ip-addr> in dotted decimal notation.                                                                      |
| <ip-addr>/<br><prefix>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.                 |
| eq                          | Equal to.                                                                                                                                                                 |
| <b>&lt;destport&gt;</b>     | The source TCP or UDP port number, specified as an integer between 0 and 65535.                                                                                           |

**Mode** IPv4 Hardware ACL Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage** First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the [access-group](#) command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the [access-list hardware \(named\)](#) command. with the required access control list number, or name, but with no further parameters selected.

Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Example** To add an access-list filter entry to access-list named my-hw-list that will permit TCP packets with a destination address of 192.168.1.1, a destination port of 80, and any source address, and source port, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-hw-list
awplus(config-ip-hw-acl)# permit tcp any 192.168.1.1/32 eq 80
```

**Related Commands** [access-list hardware \(named\)](#)  
[show running-config](#)  
[show access-list \(IPv4 Hardware ACLs\)](#)

## commit (IPv4)

**Overview** Use this command to commit the IPv4 ACL filter configuration entered at the console to the hardware immediately without exiting the IPv4 Hardware ACL Configuration mode.

This command forces the associated hardware and software IPv4 ACLs to synchronize.

**Syntax** `commit`

**Mode** IPv4 Hardware ACL Configuration

**Usage** Normally, when an IPv4 hardware ACL is edited, the new configuration state of the IPv4 ACL is not written to hardware until you exit IPv4 Hardware ACL Configuration mode. By entering this command you can ensure that the current state of a hardware access-list that is being edited is written to hardware immediately.

Scripts typically do not include the `exit` command to exit configuration modes, potentially leading to IPv4 ACL filters in hardware not being correctly updated. Using this **commit** command in a configuration script after specifying an IPv4 hardware ACL filter ensures that it is updated in the hardware immediately.

**Example** To update the hardware with the IPv4 ACL filter configuration, use the command:

```
awplus# configure terminal
awplus(config)# access-list hardware my-hw-list
awplus(config-ip-hw-acl)# commit
```

**Related Commands** [access-list hardware \(named\)](#)

# show access-list (IPv4 Hardware ACLs)

**Overview** Use this command to display the specified access-list, or all access-lists if none have been specified. Note that only defined access-lists are displayed. An error message is displayed for an undefined access-list.

**Syntax** show access-list  
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<3000-3699>|<4000-4499>|<access-list-name>]

| Parameter          | Description                                          |
|--------------------|------------------------------------------------------|
| <1-99>             | IP standard access-list.                             |
| <1300-1999>        | IP standard access-list (standard - expanded range). |
| <3000-3699>        | Hardware IP access-list.                             |
| <4000-4499>        | Hardware MAC access-list.                            |
| <access-list-name> | IP named access-list.                                |

**Mode** User Exec and Privileged Exec

**Examples** To show all access-lists configured on the switch:

```
awplus# show access-list
```

```
Standard IP access list 1
 deny 172.16.2.0, wildcard bits 0.0.0.255
Standard IP access list 20
 deny 192.168.10.0, wildcard bits 0.0.0.255
 deny 192.168.12.0, wildcard bits 0.0.0.255
Hardware IP access list 3001
 permit ip 192.168.20.0 255.255.255.0 any
Hardware IP access list 3020
 permit tcp any 192.0.2.0/24
awplus#show access-list 20
```

To show the access-list with an ID of 20:

```
awplus# show access-list 20
```

```
Standard IP access-list 20
 deny 192.168.10.0, wildcard bits 0.0.0.255
 deny 192.168.12.0, wildcard bits 0.0.0.255
```

Note the below error message if you attempt to show an undefined access-list:

```
awplus# show access-list 2
```

```
% Can't find access-list 2
```

**Related  
Commands**    [access-list \(hardware MAC numbered\)](#)  
                  [access-list hardware \(named\)](#)



# show interface access-group

**Overview** Use this command to display the access groups attached to a port. If an access group is specified, then the output only includes the ports that the specified access group is attached to. If no access group is specified then this command displays all access groups that are attached to the ports that are specified with <port-list>.

Note that **access group** is the term given for an access-list when it is applied to an interface.

**Syntax** show interface <port-list> access-group  
[<3000-3699>|<4000-4699>]

| Parameter    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <port-list>  | Specify the ports to display information. A port-list can be either: <ul style="list-style-type: none"><li>• a switch port (e.g. port1.0.6) a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.6 or port1.0.1-port1.0.6 or po1-po2</li><li>• a comma-separated list of ports and port ranges, e.g. port1.0.1,port1.0.3-1.0.6. Do not mix switch ports, static channel groups, and LACP channel groups in the same list.</li></ul> |
| access group | Select the access group whose details you want to show.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <3000-3699>  | Specifies the Hardware IP access-list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <4000-4699>  | Specifies the Hardware MAC access-list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

**Mode** User Exec and Privileged Exec

**Example** To show all access-lists attached to port1.0.1, use the command:

```
awplus# show interface port1.0.1 access-group
```

**Output** Figure 22-1: Example output from the show interface access-group command

```
Interface port1.0.1
 access-group 3000
 access-group 3002
 access-group 3001
```

**Related Commands** [access-group](#)

# 23

# IPv4 Software Access Control List (ACL) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for the IPv4 Software Access Control List (ACL) commands, and contains detailed command information and command examples about IPv4 software ACLs as applied to Routing and Multicasting, which are not applied to interfaces.

For information about ACLs, see the [ACL Feature Overview and Configuration Guide](#).

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- the [Link Aggregation Feature Overview and Configuration Guide](#).
- [Link Aggregation Commands](#)

**NOTE:** Text in parenthesis in command names indicates usage not keyword entry. For example, **access-list hardware (named)** indicates named IPv4 hardware ACLs entered as `access-list hardware <name>` where <name> is a placeholder not a keyword.

Parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as **(access-list standard numbered filter)** represents command entry in the format shown in the syntax `[<sequence-number>] {deny|permit} {<source>|host <host-address>|any}`.

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Sub-modes** Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 23-1: IPv4 Software Access List Commands and Prompts

| Command Name                           | Command Mode                    | Prompt                     |
|----------------------------------------|---------------------------------|----------------------------|
| show ip access-list                    | Privileged Exec                 | awplus#                    |
| access-group                           | Global Configuration            | awplus(config)#            |
| access-list (standard named)           | Global Configuration            | awplus(config)#            |
| access-list (standard numbered)        | Global Configuration            | awplus(config)#            |
| maximum-access-list                    | Global Configuration            | awplus(config)#            |
| (access-list standard named filter)    | IPv4 Standard ACL Configuration | awplus(config-ip-std-acl)# |
| (access-list standard numbered filter) | IPv4 Standard ACL Configuration | awplus(config-ip-std-acl)# |

- Command List**
- [“access-list extended \(named\)”](#) on page 716
  - [“access-list \(extended numbered\)”](#) on page 724
  - [“\(access-list extended ICMP filter\)”](#) on page 726
  - [“\(access-list extended IP filter\)”](#) on page 728
  - [“\(access-list extended IP protocol filter\)”](#) on page 731
  - [“\(access-list extended TCP UDP filter\)”](#) on page 736
  - [“access-list standard \(named\)”](#) on page 738
  - [“access-list \(standard numbered\)”](#) on page 740
  - [“\(access-list standard named filter\)”](#) on page 742
  - [“\(access-list standard numbered filter\)”](#) on page 744
  - [“clear ip prefix-list”](#) on page 746
  - [“ip prefix-list”](#) on page 747
  - [“maximum-access-list”](#) on page 749
  - [“show access-list \(IPv4 Software ACLs\)”](#) on page 750
  - [“show ip access-list”](#) on page 752

## access-list extended (named)

**Overview** This command configures an extended named access-list that permits or denies packets from specific source and destination IP addresses. You can either create an extended named ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Extended ACL Configuration mode for sequenced ACL filter entry after entering a list name.

The **no** variant of this command removes a specified extended named access-list.

**Syntax**  
**[list-name]** access-list extended *<list-name>*  
no access-list extended *<list-name>*

| Parameter                | Description                             |
|--------------------------|-----------------------------------------|
| <i>&lt;list-name&gt;</i> | A user-defined name for the access-list |

**Syntax [icmp]** access-list extended *<list-name>*{deny|permit} icmp *<source>* *<destination>* [icmp-type *<type-number>*] [log]  
no access-list extended *<list-name>*{deny|permit} icmp *<source>* *<destination>* [icmp-type *<type-number>*] [log]

Table 23-2: Parameters in the access-list extended (named) command - icmp

| Parameter                | Description                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------|
| <i>&lt;list-name&gt;</i> | A user-defined name for the access-list.                                                                            |
| deny                     | The access-list rejects packets that match the type, source, and destination filtering specified with this command. |
| permit                   | The access-list permits packets that match the type, source, and destination filtering specified with this command. |
| icmp                     | The access-list matches only ICMP packets.                                                                          |
| icmp-type                | Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets. |

Table 23-2: Parameters in the access-list extended (named) command - icmp

| Parameter                   | Description                                                                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>&lt;source&gt;</b>       | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                  |
| any                         | Matches any source IP address.                                                                                                                                              |
| host<ip-addr>               | Matches a single source host with the IP address given by <ip-addr> in dotted decimal notation.                                                                             |
| <ip-addr>/<br><prefix>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.                                       |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1/24. |
| <b>&lt;destination&gt;</b>  | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:   |
| any                         | Matches any destination IP address.                                                                                                                                         |
| host<ip-addr>               | Matches a single destination host with the IP address given by <ip-addr> in dotted decimal notation.                                                                        |
| <ip-addr>/<br><prefix>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                  |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1/24. |

Table 23-2: Parameters in the access-list extended (named) command - icmp

| Parameter     | Description                                                                                                                         |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------|
| <type-number> | The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type: |
| 0             | Echo replies.                                                                                                                       |
| 3             | Destination unreachable messages.                                                                                                   |
| 4             | Source quench messages.                                                                                                             |
| 5             | Redirect (change route) messages.                                                                                                   |
| 8             | Echo requests.                                                                                                                      |
| 11            | Time exceeded messages.                                                                                                             |
| 12            | Parameter problem messages.                                                                                                         |
| 13            | Timestamp requests.                                                                                                                 |
| 14            | Timestamp replies.                                                                                                                  |
| 15            | Information requests.                                                                                                               |
| 16            | Information replies.                                                                                                                |
| 17            | Address mask requests.                                                                                                              |
| 18            | Address mask replies.                                                                                                               |
| log           | Logs the results.                                                                                                                   |

**Syntax [tcp|udp]** access-list extended <list-name> {deny|permit} {tcp|udp}  
<source> eq <sourceport> <destination> eq <destport> [log]  
no access-list extended <list-name> {deny|permit} {tcp|udp}  
<source> eq <sourceport> <destination> eq <destport> [log]

Table 23-3: Parameters in the access-list extended (named) command - tcp|udp

| Parameter   | Description                                                                                                         |
|-------------|---------------------------------------------------------------------------------------------------------------------|
| <list-name> | A user-defined name for the access-list.                                                                            |
| deny        | The access-list rejects packets that match the type, source, and destination filtering specified with this command. |
| permit      | The access-list permits packets that match the type, source, and destination filtering specified with this command. |
| tcp         | The access-list matches only TCP packets.                                                                           |
| udp         | The access-list matches only UDP packets.                                                                           |

Table 23-3: Parameters in the access-list extended (named) command - tcp|udp

| Parameter                   | Description                                                                                                                                                                 |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <source>                    | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                  |
| any                         | Matches any source IP address.                                                                                                                                              |
| host<ip-addr>               | Matches a single source host with the IP address given by <ip-addr> in dotted decimal notation.                                                                             |
| <ip-addr>/<br><prefix>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.                                       |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1/24. |
| <destination>               | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:   |
| any                         | Matches any destination IP address.                                                                                                                                         |
| host<ip-addr>               | Matches a single destination host with the IP address given by <ip-addr> in dotted decimal notation.                                                                        |
| <ip-addr>/<br><prefix>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                  |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1/24. |
| <sourceport>                | The source port number, specified as an integer between 0 and 65535.                                                                                                        |
| <destport>                  | The destination port number, specified as an integer between 0 and 65535.                                                                                                   |
| eq                          | Matches port numbers equal to the port number specified immediately after this parameter.                                                                                   |
| log                         | Log the results.                                                                                                                                                            |

**Syntax** **[proto|any|ip]** access-list extended *<list-name>* {deny|permit} {proto  
*<ip-protocol>*|any|ip} {*<source>*} {*<destination>*} [log]  
no access-list extended *<list-name>*{deny|permit} {proto  
*<ip-protocol>*|any|ip}{*<source>*}{*<destination>*}[log]

Table 23-4: Parameters in the access-list extended (named) command -  
proto|ip|any

| Parameter                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |
|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|--------------------------------|-----------------------------|--------------------------------------------------------------------------------------------------------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;list-name&gt;</i>                   | A user-defined name for the access-list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |
| deny                                       | The access-list rejects packets that match the type, source, and destination filtering specified with this command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |
| permit                                     | The access-list permits packets that match the type, source, and destination filtering specified with this command.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |
| proto                                      | Matches only a specified type of IP Protocol.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |
| any                                        | The access-list matches any type of IP packet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |
| ip                                         | The access-list matches only IP packets.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |
| <i>&lt;source&gt;</i>                      | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source: <table> <tr> <td>any</td><td>Matches any source IP address.</td></tr> <tr> <td>host<i>&lt;ip-addr&gt;</i></td><td>Matches a single source host with the IP address given by <i>&lt;ip-addr&gt;</i> in dotted decimal notation.</td></tr> <tr> <td><i>&lt;ip-addr&gt;/&lt;prefix&gt;</i></td><td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td></tr> <tr> <td><i>&lt;ip-addr&gt;&lt;reverse-mask&gt;</i></td><td>Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td></tr> </table> | any | Matches any source IP address. | host <i>&lt;ip-addr&gt;</i> | Matches a single source host with the IP address given by <i>&lt;ip-addr&gt;</i> in dotted decimal notation. | <i>&lt;ip-addr&gt;/&lt;prefix&gt;</i> | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet. | <i>&lt;ip-addr&gt;&lt;reverse-mask&gt;</i> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24. |
| any                                        | Matches any source IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |
| host <i>&lt;ip-addr&gt;</i>                | Matches a single source host with the IP address given by <i>&lt;ip-addr&gt;</i> in dotted decimal notation.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |
| <i>&lt;ip-addr&gt;/&lt;prefix&gt;</i>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |
| <i>&lt;ip-addr&gt;&lt;reverse-mask&gt;</i> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |     |                                |                             |                                                                                                              |                                       |                                                                                                                                       |                                            |                                                                                                                                                           |



Table 23-4: Parameters in the access-list extended (named) command -  
proto|ip|any (cont.)

| Parameter                   | Description                                                                                                                                                                                   |
|-----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;destination&gt;</i>  | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:                     |
| any                         | Matches any destination IP address.                                                                                                                                                           |
| host<ip-addr>               | Matches a single destination host with the IP address given by <ip-addr> in dotted decimal notation.                                                                                          |
| <ip-addr>/<br><prefix>      | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                                    |
| <ip-addr><br><reverse-mask> | Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1/24.                   |
| log                         | Logs the results.                                                                                                                                                                             |
| <ip-protocol>               | The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority<br><a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a> ) |
| Protocol Number             | Protocol Description [RFC Reference]                                                                                                                                                          |
| 1                           | Internet Control Message [RFC792]                                                                                                                                                             |
| 2                           | Internet Group Management [RFC1112]                                                                                                                                                           |
| 3                           | Gateway-to-Gateway [RFC823]                                                                                                                                                                   |
| 4                           | IP in IP [RFC2003]                                                                                                                                                                            |
| 5                           | Stream [RFC1190] [RFC1819]                                                                                                                                                                    |
| 6                           | TCP (Transmission Control Protocol) [RFC793]                                                                                                                                                  |
| 8                           | EGP (Exterior Gateway Protocol) [RFC888]                                                                                                                                                      |
| 9                           | IGP (Interior Gateway Protocol) [IANA]                                                                                                                                                        |
| 11                          | Network Voice Protocol [RFC741]                                                                                                                                                               |
| 17                          | UDP (User Datagram Protocol) [RFC768]                                                                                                                                                         |
| 20                          | Host monitoring [RFC869]                                                                                                                                                                      |
| 27                          | RDP (Reliable Data Protocol) [RFC908]                                                                                                                                                         |
| 28                          | IRTP (Internet Reliable Transaction Protocol) [RFC938]                                                                                                                                        |
| 29                          | ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]                                                                                                                                             |
| 30                          | Bulk Data Transfer Protocol [RFC969]                                                                                                                                                          |

Table 23-4: Parameters in the access-list extended (named) command -  
proto|ip|any (cont.)

| Parameter                | Description                                                |
|--------------------------|------------------------------------------------------------|
| <ip-protocol><br>(cont.) | Protocol Number      Protocol Description [RFC Reference]  |
|                          | 33      Datagram Congestion Control Protocol [RFC4340]     |
|                          | 48      DSR (Dynamic Source Routing Protocol) [RFC4728]    |
|                          | 50      ESP (Encap Security Payload) [RFC2406]             |
|                          | 51      AH (Authentication Header) [RFC2402]               |
|                          | 54      NARP (NBMA Address Resolution Protocol) [RFC1735]  |
|                          | 88      EIGRP (Enhanced Interior Gateway Routing Protocol) |
|                          | 89      OSPFIGP [RFC1583]                                  |
|                          | 97      Ethernet-within-IP Encapsulation / RFC3378         |
|                          | 98      Encapsulation Header / RFC1241                     |
|                          | 108      IP Payload Compression Protocol / RFC2393         |
|                          | 112      Virtual Router Redundancy Protocol / RFC3768      |
|                          | 134      RSVP-E2E-IGNORE / RFC3175                         |
|                          | 135      Mobility Header / RFC3775                         |
|                          | 136      UDPLite / RFC3828                                 |
|                          | 137      MPLS-in-IP / RFC4023                              |
|                          | 138      MANET Protocols / RFC-ietf-manet-iana-07.txt      |
|                          | 139 - 252      Unassigned / IANA                           |
|                          | 253      Use for experimentation and testing / RFC3692     |
|                          | 254      Use for experimentation and testing / RFC3692     |
|                          | 255      Reserved / IANA                                   |

**Mode** Global Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** Use this command when configuring access-list for filtering IP software packets. To enable backwards compatibility you can either create access-lists from within this command, or you can enter **access-list** followed by only the number. This latter

method moves you to the IPv4 Extended ACL Configuration mode for the selected access-list number, and from here you can configure your access-lists by using the commands ([access-list extended ICMP filter](#)), ([access-list extended IP filter](#)), and ([access-list extended IP protocol filter](#)).

The table [IPv4 Software Access List Commands and Prompts](#) on page 715 shows the prompts at which ACL commands are entered.

Note that packets must match both the source and the destination details.

**NOTE:** Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Examples** You can enter the extended named ACL in the Global Configuration mode together with the ACL filter entry on the same line, as shown below:

```
awplus# configure terminal
```

```
awplus(config)# access-list extended TK deny tcp 2.2.2.3/24 eq
14 3.3.3.4/24 eq 12 log
```

Alternatively, you can enter the extended named ACL in Global Configuration mode before specifying the ACL filter entry in the IPv4 Extended ACL Configuration mode, as shown below:

```
awplus# configure terminal
```

```
awplus(config)# access-list extended TK
```

```
awplus(config-ip-ext-acl)# deny tcp 2.2.2.3/24 eq 14 3.3.3.4/24
eq 12 log
```

## access-list (extended numbered)

**Overview** This command configures an extended numbered access-list that permits or denies packets from specific source and destination IP addresses. You can either create an extended numbered ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Extended ACL Configuration mode for sequenced ACL filter entry after entering a list number.

The **no** variant of this command removes a specified extended named access-list.

**Syntax [list-number]** `access-list {<100-199>|<2000-2699>}`  
`no access-list {<100-199>|<2000-2699>}`

| Parameter   | Description                               |
|-------------|-------------------------------------------|
| <100-199>   | IP extended access-list.                  |
| <2000-2699> | IP extended access-list (expanded range). |

**Syntax [deny|permit]** `access-list {<100-199>|<2000-2699>} {deny|permit} ip <source> <destination>`  
`no access-list {<100-199>|<2000-2699>} {deny|permit} ip <source> <destination>`

| Parameter                   | Description                                                                                                                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <100-199>                   | IP extended access-list.                                                                                                                                                                                                 |
| <2000-2699>                 | IP extended access-list (expanded range).                                                                                                                                                                                |
| deny                        | Access-list rejects packets that match the source and destination filtering specified with this command.                                                                                                                 |
| permit                      | Access-list permits packets that match the source and destination filtering specified with this command.                                                                                                                 |
| <source>                    | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                                                               |
| any                         | Matches any source IP address.                                                                                                                                                                                           |
| host<ip-addr>               | Matches a single source host with the IP address given by <ip-addr> in dotted decimal notation.                                                                                                                          |
| <ip-addr><br><reverse-mask> | An IPv4 address, followed by a reverse mask in dotted decimal format. For example, entering 192.168.1.10.0.0.255 is the same as entering 192.168.1.1/24. This matches any source IP address within the specified subnet. |

| Parameter                   | Description                                                                                                                                                                                                                                       |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <destination>               | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:                                                                         |
| any                         | Matches any destination IP address.                                                                                                                                                                                                               |
| host<ip-addr>               | Matches a single destination host with the IP address given by <ip-addr> in dotted decimal notation.                                                                                                                                              |
| <ip-addr><br><reverse-mask> | An IPv4 address, followed by a reverse mask in dotted decimal format. For example, entering 192 . 168 . 1 . 1 0 . 0 . 0 . 255 is the same as entering 192 . 168 . 1 . 1 /24. This matches any destination IP address within the specified subnet. |

**Mode** Global Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** Use this command when configuring access-list for filtering IP software packets. To enable backwards compatibility you can either create access-lists from within this command, or you can enter **access-list** followed by only the number. This latter method moves you to the IPv4 Extended ACL Configuration mode for the selected access-list number, and from here you can configure your access-lists by using the commands ([access-list extended ICMP filter](#)), ([access-list extended IP filter](#)), and ([access-list extended IP protocol filter](#)).

The table [IPv4 Software Access List Commands and Prompts](#) shows the prompts at which ACL commands are entered. See the relevant links shown for the **Related Commands**.

Note that packets must match both the source and the destination details.

**NOTE:** Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Examples** You can enter the extended named ACL in the Global Configuration mode together with the ACL filter entry on the same line, as in previous software releases as shown below:

```
awplus# configure terminal
awplus(config)# access-list 101 deny ip 172.16.10.0 0.0.0.255
any
```

Alternatively, you can enter the extended named ACL in Global Configuration mode before specifying the ACL filter entry in the IPv4 Extended ACL Configuration mode, as shown below:

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)# deny ip 172.16.10.0 0.0.0.255 any
```

## (access-list extended ICMP filter)

**Overview** Use this ACL filter to add a new ICMP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an ICMP filter entry from the current extended access-list. You can specify the ICMP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its ICMP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the [show access-list \(IPv4 Software ACLs\)](#) command.

**Syntax [icmp]** [*<sequence-number>*] {deny|permit} icmp *<source>* *<destination>*  
[icmp-type *<icmp-value>*] [log]  
  
no {deny|permit} icmp *<source>* *<destination>*[icmp-type  
*<icmp-value>*] [log]  
  
no *<sequence-number>*

| Parameter                      | Description                                                                                                                                                                      |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;sequence-number&gt;</i> | <i>&lt;1-65535&gt;</i><br>The sequence number for the filter entry of the selected access control list.                                                                          |
| deny                           | Access-list rejects packets that match the source and destination filtering specified with this command.                                                                         |
| permit                         | Access-list permits packets that match the source and destination filtering specified with this command.                                                                         |
| icmp                           | ICMP packet type.                                                                                                                                                                |
| <i>&lt;source&gt;</i>          | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                       |
|                                | <i>&lt;ip-addr&gt;/&lt;prefix&gt;</i> An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.      |
|                                | any      Matches any source IP address.                                                                                                                                          |
| <i>&lt;destination&gt;</i>     | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:        |
|                                | <i>&lt;ip-addr&gt;/&lt;prefix&gt;</i> An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet. |
|                                | any      Matches any destination IP address.                                                                                                                                     |
| icmp-type                      | The ICMP type.                                                                                                                                                                   |

| Parameter    | Description                 |
|--------------|-----------------------------|
| <icmp-value> | The value of the ICMP type. |
| log          | Log the results.            |

**Mode** IPv4 Extended ACL Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the [access-list \(extended numbered\)](#) command or the [access-list extended \(named\)](#) command, with the required access control list number, or name - but with no further parameters selected.

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Examples** To add a new entry in access-list called my-list that will reject ICMP packets from 10.0.0.1 to 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny icmp 10.0.0.1/32 192.168.1.1/32
```

Use the following commands to add a new filter at sequence number 5 position of the access-list called my-list. The filter will accept the ICMP type 8 packets from 10.1.1.0/24 network, to 192.168.1.0 network:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit icmp 10.1.1.0/24
192.168.1.0/24 icmp-type 8
```

## (access-list extended IP filter)

**Overview** Use this ACL filter to add a new IP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP filter entry from the current extended access-list. You can specify the IP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the [show access-list \(IPv4 Software ACLs\)](#) command.

**Syntax [ip]** [*<sequence-number>*] {deny|permit} ip *<source>* *<destination>*  
`no` {deny|permit} ip *<source>* *<destination>*  
`no` *<sequence-number>*

| Parameter                      | Description                                                                                                                                                                               |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;sequence-number&gt;</i> | <i>&lt;1-65535&gt;</i><br>The sequence number for the filter entry of the selected access control list.                                                                                   |
| deny                           | Access-list rejects packets that match the source and destination filtering specified with this command.                                                                                  |
| permit                         | Access-list permits packets that match the source and destination filtering specified with this command.                                                                                  |
| <i>&lt;source&gt;</i>          | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                                |
|                                | any                      Matches any source IP address.                                                                                                                                   |
|                                | host <i>&lt;ip-addr&gt;</i> Matches a single source host with the IP address given by <i>&lt;ip-addr&gt;</i> in dotted decimal notation.                                                  |
|                                | <i>&lt;ip-addr&gt;</i><br><i>&lt;reverse-mask&gt;</i> Alternatively, enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, enter 192.168.1.1 0.0.0.255. |



| Parameter                   | Description                                                                                                                                                               |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <destination>               | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination: |
| any                         | Matches any destination IP address.                                                                                                                                       |
| host<ip-addr>               | Matches a single destination host with the IP address given by <ip-addr> in dotted decimal notation.                                                                      |
| <ip-addr><br><reverse-mask> | Alternatively, enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, enter 192.168.1.1 0.0.0.255.                                       |

**Mode** Extended ACL Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the [access-list \(extended numbered\)](#) command or the [access-list extended \(named\)](#) command, with the required access control list number, or name - but with no further parameters selected.

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Example 1 [list-number]** First use the following commands to enter the IPv4 Extended ACL Configuration mode and define a numbered extended access-list 101:

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)#
```

Then use the following commands to add a new entry to the numbered extended access-list 101 that will reject packets from 10.0.0.1 to 192.168.1.1:

```
awplus(config-ip-ext-acl)# deny ip host 10.0.0.1 host
192.168.1.1
awplus(config-ip-ext-acl)# 20 permit ip any any
```

**Example 2 [list-name]** First use the following commands to enter the IPv4 Extended ACL Configuration mode and define a named access-list called my-acl:

```
awplus# configure terminal
awplus(config)# access-list extended my-acl
awplus(config-ip-ext-acl)#
```

Then use the following commands to add a new entry to the named access-list `my-acl` that will reject packets from `10.0.0.1` to `192.168.1.1`:

```
awplus(config-ip-ext-acl)# deny ip host 10.0.0.1 host
192.168.1.1
```

```
awplus(config-ip-ext-acl)# 20 permit ip any any
```

**Example 3** Use the following commands to remove the access-list filter entry with sequence  
**[list-number]** number 20 from extended numbered access-list 101.

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)# no 20
```

**Example 4** Use the following commands to remove the access-list filter entry with sequence  
**[list-name]** number 20 from extended named access-list `my-acl`:

```
awplus# configure terminal
awplus(config)# access-list extended my-acl
awplus(config-ip-ext-acl)# no 20
```

## (access-list extended IP protocol filter)

**Overview** Use this ACL filter to add a new IP protocol type filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP protocol filter entry from the current extended access-list. You can specify the IP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the [show access-list \(IPv4 Software ACLs\)](#) command.

**Syntax [proto]** [*<sequence-number>*] {deny|permit} proto *<ip-protocol>* *<source>* *<destination>* [log]  
`no` {deny|permit} proto *<ip-protocol>* *<source>* *<destination>* [log]  
`no` *<sequence-number>*

| Parameter                        | Description                                                                                              |
|----------------------------------|----------------------------------------------------------------------------------------------------------|
| <i>&lt;sequence-number&gt;</i>   | <i>&lt;1-65535&gt;</i><br>The sequence number for the filter entry of the selected access control list.  |
| deny                             | Access-list rejects packets that match the source and destination filtering specified with this command. |
| permit                           | Access-list permits packets that match the source and destination filtering specified with this command. |
| proto <i>&lt;ip-protocol&gt;</i> | The IP Protocol type specified by its protocol number <i>&lt;1-255&gt;</i> .                             |

| Parameter     | Description                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-protocol> | The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority <a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a> ). |
|               | Protocol Number      Protocol Description [RFC Reference]                                                                                                                                   |
|               | 1      Internet Control Message [RFC792]                                                                                                                                                    |
|               | 2      Internet Group Management [RFC1112]                                                                                                                                                  |
|               | 3      Gateway-to-Gateway [RFC823]                                                                                                                                                          |
|               | 4      IP in IP [RFC2003]                                                                                                                                                                   |
|               | 5      Stream [RFC1190] [RFC1819]                                                                                                                                                           |
|               | 6      TCP (Transmission Control Protocol) [RFC793]                                                                                                                                         |
|               | 8      EGP (Exterior Gateway Protocol) [RFC888]                                                                                                                                             |
|               | 9      IGP (Interior Gateway Protocol) [IANA]                                                                                                                                               |
|               | 11      Network Voice Protocol [RFC741]                                                                                                                                                     |

| Parameter                | Description                                               |
|--------------------------|-----------------------------------------------------------|
| <ip-protocol><br>(cont.) | 17 UDP (User Datagram Protocol) [RFC768]                  |
|                          | 20 Host monitoring [RFC869]                               |
|                          | 27 RDP (Reliable Data Protocol) [RFC908]                  |
|                          | 28 IRTP (Internet Reliable Transaction Protocol) [RFC938] |
|                          | 29 ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]      |
|                          | 30 Bulk Data Transfer Protocol [RFC969]                   |
|                          | 33 DCCP (Datagram Congestion Control Protocol) [RFC4340]  |
|                          | 48 DSR (Dynamic Source Routing Protocol) [RFC4728]        |
|                          | 50 ESP (Encap Security Payload) [RFC2406]                 |
|                          | 51 AH (Authentication Header) [RFC2402]                   |
|                          | 54 NARP (NBMA Address Resolution Protocol) [RFC1735]      |
|                          | 88 EIGRP (Enhanced Interior Gateway Routing Protocol)     |
|                          | 89 OSPFIGP [RFC1583]                                      |
|                          | 97 Ethernet-within-IP Encapsulation / RFC3378             |
|                          | 98 Encapsulation Header / RFC1241                         |
|                          | 108 IP Payload Compression Protocol / RFC2393             |
|                          | 112 Virtual Router Redundancy Protocol / RFC3768          |
|                          | 134 RSVP-E2E-IGNORE / RFC3175                             |
|                          | 135 Mobility Header / RFC3775                             |
|                          | 136 UDPLite / RFC3828                                     |
|                          | 137 MPLS-in-IP / RFC4023                                  |
|                          | 138 MANET Protocols / RFC-ietf-manet-iana-07.txt          |
|                          | 139-252 Unassigned / IANA                                 |
|                          | 253 Use for experimentation and testing / RFC3692         |
|                          | 254 Use for experimentation and testing / RFC3692         |
|                          | 255 Reserved / IANA                                       |

| Parameter     | Description                                                                                                                                                               |                                                                                                                                            |
|---------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <source>      | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                |                                                                                                                                            |
|               | <ip-addr>/<br><prefix>                                                                                                                                                    | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.      |
|               | any                                                                                                                                                                       | Matches any source IP address.                                                                                                             |
| <destination> | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination: |                                                                                                                                            |
|               | <ip-addr>/<br><prefix>                                                                                                                                                    | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet. |
|               | any                                                                                                                                                                       | Matches any destination IP address.                                                                                                        |
| log           | Log the results.                                                                                                                                                          |                                                                                                                                            |

**Mode** IPv4 Extended ACL Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the [access-list \(extended numbered\)](#) command or the [access-list extended \(named\)](#) command, with the required access control list number, or name - but with no further parameters selected.

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Example 1 [creating a list]** Use the following commands to add a new access-list filter entry to the access-list named my - list that will reject IP packets from source address 10 . 10 . 1 . 1/32 to destination address 192 . 68 . 1 . 1/32:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny ip 10.10.1.1/32 192.168.1.1/32
```

**Example 2** Use the following commands to add a new access-list filter entry at sequence  
**[adding to a list]** position 5 in the access-list named my - list that will accept packets from source  
address 10.10.1.1/24 to destination address 192.68.1.1/24:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit ip 10.10.1.1/24
192.168.1.1/ 24
```

## (access-list extended TCP UDP filter)

**Overview** Use this ACL filter to add a new TCP or UDP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a TCP or UDP filter entry from the current extended access-list. You can specify the TCP or UDP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its TCP or UDP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the [show access-list \(IPv4 Software ACLs\)](#) command.

**Syntax [tcp|udp]** [*<sequence-number>*] {deny|permit} {tcp|udp} *<source>* eq *<sourceport>* *<destination>* eq *<destport>* [log]  
no [*<sequence-number>*] {deny|permit} {tcp|udp} *<source>* eq *<sourceport>* *<destination>* eq *<destport>* [log]  
no [*<sequence-number>*]

| Parameter                      | Description                                                                                                                                                                      |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;sequence-number&gt;</i> | <i>&lt;1-65535&gt;</i><br>The sequence number for the filter entry of the selected access control list.                                                                          |
| deny                           | Access-list rejects packets that match the source and destination filtering specified with this command.                                                                         |
| permit                         | Access-list permits packets that match the source and destination filtering specified with this command.                                                                         |
| tcp                            | The access-list matches only TCP packets.                                                                                                                                        |
| udp                            | The access-list matches only UDP packets.                                                                                                                                        |
| <i>&lt;source&gt;</i>          | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:                       |
|                                | <i>&lt;ip-addr&gt;/<br/>&lt;prefix&gt;</i> An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet. |
|                                | any      Matches any source IP address.                                                                                                                                          |
| <i>&lt;sourceport&gt;</i>      | The source port number, specified as an integer between 0 and 65535.                                                                                                             |



| Parameter              | Description                                                                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <destination>          | The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination: |
| <ip-addr>/<br><prefix> | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                |
| any                    | Matches any destination IP address.                                                                                                                                       |
| <destport>             | The destination port number, specified as an integer between 0 and 65535.                                                                                                 |
| eq                     | Matches port numbers equal to the port number specified immediately after this parameter.                                                                                 |
| log                    | Log the results.                                                                                                                                                          |

**Mode** IPv4 Extended ACL Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** The access control list being configured is selected by running the [access-list \(extended numbered\)](#) command or the [access-list extended \(named\)](#) command, with the required access control list number, or name - but with no further parameters selected.

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Example 1 [creating a list]** To add a new entry to the access-list named my - list that will reject TCP packets from 10.0.0.1 on TCP port 10 to 192.168.1.1 on TCP port 20, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny tcp 10.0.0.1/32 eq 10
192.168.1.1/32 eq 20
```

**Example 2 [adding to a list]** To insert a new entry with sequence number 5 of the access-list named my - list that will accept UDP packets from 10.1.1.0/24 network to 192.168.1.0/24 network on UDP port 80, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit udp 10.1.1.0/24
192.168.1.0/24 eq 80
```

## access-list standard (named)

**Overview** This command configures a standard named access-list that permits or denies packets from a specific source IP address. You can either create a standard named ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Standard ACL Configuration mode for sequenced ACL filter entry after first entering an access-list name.

The **no** variant of this command removes a specified standard named access-list.

**Syntax**  
**[list-name]** access-list standard <standard-access-list-name>  
no access-list standard <standard-access-list-name>

| Parameter                   | Description                                  |
|-----------------------------|----------------------------------------------|
| <standard-access-list-name> | Specify a name for the standard access-list. |

**Syntax**  
**[deny|permit]** access-list standard <standard-access-list-name> {deny|permit} <source>  
no access-list standard <standard-access-list-name> {deny|permit} <source>

| Parameter                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                          |                    |                                                                                                                                       |     |                                |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------------------------------------------------------------------------|-----|--------------------------------|
| <standard-access-list-name> | Specify a name for the standard access-list.                                                                                                                                                                                                                                                                                                                                                                                         |                    |                                                                                                                                       |     |                                |
| deny                        | The access-list rejects packets that match the source filtering specified with this command.                                                                                                                                                                                                                                                                                                                                         |                    |                                                                                                                                       |     |                                |
| permit                      | The access-list permits packets that match the source filtering specified with this command.                                                                                                                                                                                                                                                                                                                                         |                    |                                                                                                                                       |     |                                |
| <source>                    | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source: <table><tr><td>&lt;ip-addr&gt;/&lt;prefix&gt;</td><td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.</td></tr><tr><td>any</td><td>Matches any source IP address.</td></tr></table> | <ip-addr>/<prefix> | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet. | any | Matches any source IP address. |
| <ip-addr>/<prefix>          | An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.                                                                                                                                                                                                                                                                                                |                    |                                                                                                                                       |     |                                |
| any                         | Matches any source IP address.                                                                                                                                                                                                                                                                                                                                                                                                       |                    |                                                                                                                                       |     |                                |

**Mode** Global Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** Use this command when configuring a standard named access-list for filtering IP software packets. For backwards compatibility you can either create the access-list from within this command, or you can enter this command followed by only the standard access-list name then enter. This latter method moves you to the IPv4 Standard ACL Configuration mode for the selected standard named access-list, and from here you can configure the deny or permit filters for this selected standard named access-list.

See the table [IPv4 Software Access List Commands and Prompts](#) which shows the prompts at which ACL commands are entered. See the relevant links shown for the **Related Commands**.

**NOTE:** Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Examples** To define a standard access-list named `my-list` and deny any packets from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard my-list deny any
```

Alternatively, to define a standard access-list named `my-list` and enter the IPv4 Standard ACL Configuration mode to deny any packets from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# 5 deny any
```

**Related Commands** [\(access-list standard named filter\)](#)  
[show running-config](#)  
[show ip access-list](#)

## access-list (standard numbered)

**Overview** This command configures a standard numbered access-list that permits or denies packets from a specific source IP address. You can either create a standard numbered ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Standard ACL Configuration mode for sequenced ACL filter entry after first entering an access-list number.

The **no** variant of this command removes a specified standard numbered access-list.

**Syntax**  
**[list-number]** access-list {<1-99>|<1300-1999>}  
no access-list {<1-99>|<1300-1999>}

| Parameter   | Description                               |
|-------------|-------------------------------------------|
| <1-99>      | IP standard access-list.                  |
| <1300-1999> | IP standard access-list (expanded range). |

**Syntax [deny|permit]** access-list {<1-99>|<1300-1999>} {deny|permit} <source>  
no access-list {<1-99>|<1300-1999>} {deny|permit} <source>

| Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |           |                                                                                                                                                                |                |  |     |                                |
|----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|--|-----|--------------------------------|
| <1-99>         | IP standard access-list.                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |           |                                                                                                                                                                |                |  |     |                                |
| <1300-1999>    | IP standard access-list (expanded range).                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |                                                                                                                                                                |                |  |     |                                |
| deny           | Access-list rejects packets from the specified source.                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |                                                                                                                                                                |                |  |     |                                |
| permit         | Access-list accepts packets from the specified source.                                                                                                                                                                                                                                                                                                                                                                                                                                        |           |                                                                                                                                                                |                |  |     |                                |
| <source>       | The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source: <table><tr><td>&lt;ip-addr&gt;</td><td>Enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.</td></tr><tr><td>&lt;reverse-mask&gt;</td><td></td></tr><tr><td>any</td><td>Matches any source IP address.</td></tr></table> | <ip-addr> | Enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24. | <reverse-mask> |  | any | Matches any source IP address. |
| <ip-addr>      | Enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, entering 192.168.1.1 0.0.0.255 is the same as entering 192.168.1.1/24.                                                                                                                                                                                                                                                                                                                                |           |                                                                                                                                                                |                |  |     |                                |
| <reverse-mask> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |           |                                                                                                                                                                |                |  |     |                                |
| any            | Matches any source IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                                |           |                                                                                                                                                                |                |  |     |                                |

**Mode** Global Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** Use this command when configuring a standard numbered access-list for filtering IP software packets. For backwards compatibility you can either create the access-list from within this command, or you can enter this command followed by

only the standard access-list name. This moves you to the IPv4 Standard ACL Configuration mode for the selected standard numbered access-list, and from here you can configure the deny or permit filters for this selected standard numbered access-list.

The table [IPv4 Software Access List Commands and Prompts](#) shows the prompts at which ACL commands are entered.

**NOTE:** Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Examples** To create ACL number 67 that will deny packets from subnet 172 . 16 . 10, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 67 deny 172.16.10.0 0.0.0.255
```

Alternatively, to enter the IPv4 Standard ACL Configuration mode to create the ACL filter and deny packets from subnet 172 . 16 . 10 . 0 for the standard numbered access-list 67, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 67
awplus(config-ip-std-acl)# deny 172.16.10.0 0.0.0.255
```

**Related Commands** [\(access-list standard named filter\)](#)  
[show running-config](#)  
[show ip access-list](#)

## (access-list standard named filter)

**Overview** This ACL filter adds a source IP address filter entry to a current named standard access-list. If the sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a source IP address filter entry from the current named standard access-list. You can specify the source IP address filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its source IP address filter profile without specifying its sequence number.

Note that the sequence number can be found by running the [show access-list \(IPv4 Software ACLs\)](#) command.

**Syntax** [`<sequence-number>`] {deny|permit} {<source> [exact-match]|any}  
no {deny|permit} {<source> [exact-match]|any}  
no <sequence-number>

| Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                                                                                                                            |           |                                    |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------------------------|
| <sequence-number>  | <1-65535><br>The sequence number for the filter entry of the selected access control list.                                                                                                                                                                                                                                                                                                                                                       |                    |                                                                                                                                            |           |                                    |
| deny               | Access-list rejects packets of the source filtering specified.                                                                                                                                                                                                                                                                                                                                                                                   |                    |                                                                                                                                            |           |                                    |
| permit             | Access-list allows packets of the source filtering specified                                                                                                                                                                                                                                                                                                                                                                                     |                    |                                                                                                                                            |           |                                    |
| <source>           | The source address of the packets. You can specify either a subnet or all sources. The following are the valid formats for specifying the source: <table><tr><td>&lt;ip-addr&gt;/&lt;prefix&gt;</td><td>An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.</td></tr><tr><td>&lt;ip-addr&gt;</td><td>An IPv4 address in a.b.c.d format.</td></tr></table> | <ip-addr>/<prefix> | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet. | <ip-addr> | An IPv4 address in a.b.c.d format. |
| <ip-addr>/<prefix> | An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.                                                                                                                                                                                                                                                                                                       |                    |                                                                                                                                            |           |                                    |
| <ip-addr>          | An IPv4 address in a.b.c.d format.                                                                                                                                                                                                                                                                                                                                                                                                               |                    |                                                                                                                                            |           |                                    |
| exact-match        | Specify an exact IP prefix to match on.                                                                                                                                                                                                                                                                                                                                                                                                          |                    |                                                                                                                                            |           |                                    |
| any                | Matches any source IP address.                                                                                                                                                                                                                                                                                                                                                                                                                   |                    |                                                                                                                                            |           |                                    |

**Mode** IPv4 Standard ACL Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** *The access control list being configured is selected by running the [access-list standard \(named\)](#) command with the required access control list number, or name, but with no further parameters selected.*

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Examples** Use the following commands to add a new filter entry to access-list my-list that will reject IP address 10.1.1.1:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# deny 10.1.1.1/32
```

Use the following commands to insert a new filter entry into access-list my-list at sequence position number 15 that will accept IP network 10.1.2.0:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# 15 permit 10.1.2.0/24
```

**Related Commands** [access-list standard \(named\)](#)  
[show running-config](#)  
[show ip access-list](#)

## (access-list standard numbered filter)

**Overview** This ACL filter adds a source IP address filter entry to a current standard numbered access-list. If a sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new filter entry is added at the end of the access-list.

The **no** variant of this command removes a source IP address filter entry from the current standard numbered access-list. You can specify the source IP address filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its source IP address filter profile without specifying its sequence number.

Note that the sequence number can be found by running the [show access-list \(IPv4 Software ACLs\)](#) command.

**Syntax** [`<sequence-number>`] {deny|permit} {<source>|host  
<host-address>|any}  
no {deny|permit} {<source>|host <host-address>|any}  
no <sequence-number>

| Parameter                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                             |                                                                                                                                                            |           |                                    |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------------------------------|
| <sequence-number>           | <1-65535><br>The sequence number for the filter entry of the selected access control list.                                                                                                                                                                                                                                                                                                                                                                                    |                             |                                                                                                                                                            |           |                                    |
| deny                        | Access-list rejects packets of the type specified.                                                                                                                                                                                                                                                                                                                                                                                                                            |                             |                                                                                                                                                            |           |                                    |
| permit                      | Access-list allows packets of the type specified                                                                                                                                                                                                                                                                                                                                                                                                                              |                             |                                                                                                                                                            |           |                                    |
| <source>                    | The source address of the packets. You can specify either a subnet or all sources. The following are the valid formats for specifying the source:<br><table><tr><td>&lt;ip-addr&gt;<br/>&lt;reverse-mask&gt;</td><td>Enter a reverse mask for the source address in dotted decimal format. For example, entering 192.168.1.10.0.0.0.255 is the same as entering 192.168.1.1/24.</td></tr><tr><td>&lt;ip-addr&gt;</td><td>An IPv4 address in a.b.c.d format.</td></tr></table> | <ip-addr><br><reverse-mask> | Enter a reverse mask for the source address in dotted decimal format. For example, entering 192.168.1.10.0.0.0.255 is the same as entering 192.168.1.1/24. | <ip-addr> | An IPv4 address in a.b.c.d format. |
| <ip-addr><br><reverse-mask> | Enter a reverse mask for the source address in dotted decimal format. For example, entering 192.168.1.10.0.0.0.255 is the same as entering 192.168.1.1/24.                                                                                                                                                                                                                                                                                                                    |                             |                                                                                                                                                            |           |                                    |
| <ip-addr>                   | An IPv4 address in a.b.c.d format.                                                                                                                                                                                                                                                                                                                                                                                                                                            |                             |                                                                                                                                                            |           |                                    |
| host                        | A single source host.                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                             |                                                                                                                                                            |           |                                    |
| <host-address>              | Single source host address.                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                             |                                                                                                                                                            |           |                                    |
| any                         | Matches any source IP address.                                                                                                                                                                                                                                                                                                                                                                                                                                                |                             |                                                                                                                                                            |           |                                    |

**Mode** IPv4 Standard ACL Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.



**Usage** An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

**NOTE:** *The access control list being configured is selected by running the [access-list standard \(named\)](#) command with the required access control list number, or name, but with no further parameters selected.*

Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Example** To add a new entry accepting the IP network 10.1.1.0/24 at the sequence number 15 position, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 99
awplus(config-ip-std-acl)# 15 permit 10.1.2.0 0.0.0.255
```

**Related Commands** [access-list \(standard numbered\)](#)  
[show running-config](#)  
[show ip access-list](#)

# 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
```

# 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** 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 below 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
```

# maximum-access-list

**Overview** Sets the maximum number of filters that can be added to any access-list. These are access-lists within the ranges <1-199>, <1300-1999> and <2000-2699> and named standard and extended access-lists.

The **no** variant of this command removes the limit on the number of filters that can be added to a software access-list

**Syntax** maximum-access-list <1-4294967294>  
no maximum-access-list

| Parameter        | Description   |
|------------------|---------------|
| <1 - 4294967294> | Filter range. |

**Mode** Global Configuration

**Example** To set the maximum number of software filters to 200:

```
awplus# configure terminal
awplus(config)# maximum-access-list 200
```

# show access-list (IPv4 Software ACLs)

**Overview** Use this command to display the specified access-list, or all access-lists if none have been specified. Note that only defined access-lists are displayed. An error message is displayed for an undefined access-list

**Syntax** show access-list  
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<3000-3699>|<4000-4499>|<access-list-name>]

| Parameter          | Description                                          |
|--------------------|------------------------------------------------------|
| <1-99>             | IP standard access-list.                             |
| <100-199>          | IP extended access-list.                             |
| <1300-1999>        | IP standard access-list (standard - expanded range). |
| <2000-2699>        | IP extended access-list (extended - expanded range). |
| <3000-3699>        | Hardware IP access-list.                             |
| <4000-4499>        | Hardware MAC access-list.                            |
| <access-list-name> | IP named access-list.                                |

**Mode** User Exec and Privileged Exec

**Examples** To show all access-lists configured on the switch:

```
awplus# show access-list
```

```
Standard IP access list 1
 deny 172.16.2.0, wildcard bits 0.0.0.255
Standard IP access list 20
 deny 192.168.10.0, wildcard bits 0.0.0.255
 deny 192.168.12.0, wildcard bits 0.0.0.255
Hardware IP access list 3001
 permit ip 192.168.20.0 255.255.255.0 any
Hardware IP access list 3020
 permit tcp any 192.0.2.0/24
awplus#show access-list 20
```

To show the access-list with an ID of 20:

```
awplus# show access-list 20
```

```
Standard IP access-list 20
 deny 192.168.10.0, wildcard bits 0.0.0.255
 deny 192.168.12.0, wildcard bits 0.0.0.255
```

Note the below error message if you attempt to show an undefined access-list:

```
awplus# show access-list 2
```

```
% Can't find access-list 2
```

**Related  
Commands**

[access-list standard \(named\)](#)

[access-list \(standard numbered\)](#)

[access-list \(extended numbered\)](#)

# show ip access-list

**Overview** Use this command to display IP access-lists.

**Syntax** show ip access-list  
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<access-list-name>]

| Parameter          | Description                               |
|--------------------|-------------------------------------------|
| <1-99>             | IP standard access-list.                  |
| <100-199>          | IP extended access-list.                  |
| <1300-1999>        | IP standard access-list (expanded range). |
| <2000-2699>        | IP extended access-list (expanded range). |
| <access-list-name> | IP named access-list.                     |

**Mode** User Exec and Privileged Exec

**Example** awplus# show ip access-list

**Output** Figure 23-1: Example output from the **show ip access-list** command

```
Standard IP access-list 1
 permit 172.168.6.0, wildcard bits 0.0.0.255
 permit 192.168.6.0, wildcard bits 0.0.0.255
```



# 24

# IPv6 Hardware Access Control List (ACL) Commands

## Introduction

**Overview** IPv6 Hardware ACLs are supported in Software Version 5.4.3A-1.x and later.

This chapter provides an alphabetical reference for the IPv6 Hardware Access Control List (ACL) commands, and contains detailed command information and command examples about IPv6 hardware ACLs, which are applied directly to interfaces using the [ipv6 traffic-filter](#) command.

For information about ACLs, see the [ACL Feature Overview and Configuration Guide](#).

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- the [Link Aggregation Feature Overview and Configuration Guide](#).
- [Link Aggregation Commands](#)

Note that text in parenthesis in command names indicates usage not keyword entry. For example, **ipv6-access-list (named)** indicates named IPv6 ACLs entered as `ipv6-access-list <name>` where *<name>* is a placeholder not a keyword.

Note also that parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as **(ipv6 access-list standard IPv6 filter)** represents command entry in the format shown in the syntax `[<sequence-number>] {deny|permit} [<IPv6-source-address/prefix-length>|any]`.

**NOTE:** Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

IPv6 Hardware ACLs are supported in Software Version 5.4.3A-1.x and later.

**Sub-modes** Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 24-1: IPv6 Hardware Access List Commands and Prompts

| Command Name                                               | Command Mode                    | Prompt                      |
|------------------------------------------------------------|---------------------------------|-----------------------------|
| <a href="#">show ipv6 access-list (IPv6 Hardware ACLs)</a> | Privileged Exec                 | awplus#                     |
| <a href="#">ipv6 access-list (named)</a>                   | Global Configuration            | awplus(config)#             |
| <a href="#">(ipv6 access-list named ICMP filter)</a>       | Global Configuration            | awplus(config)#             |
| <a href="#">ipv6 traffic-filter</a>                        | Interface Configuration         | awplus(config-if)#          |
| <a href="#">commit (IPv6)</a>                              | IPv6 Hardware ACL Configuration | awplus(config-ipv6-hw-acl)# |
| <a href="#">(ipv6 access-list named ICMP filter)</a>       | IPv6 Hardware ACL Configuration | awplus(config-ipv6-hw-acl)# |
| <a href="#">(ipv6 access-list named protocol filter)</a>   | IPv6 Hardware ACL Configuration | awplus(config-ipv6-hw-acl)# |
| <a href="#">(ipv6 access-list named TCP UDP filter)</a>    | IPv6 Hardware ACL Configuration | awplus(config-ipv6-hw-acl)# |

- Command List**
- [“commit \(IPv6\)”](#) on page 755
  - [“ipv6 access-list \(named\)”](#) on page 756
  - [“\(ipv6 access-list named ICMP filter\)”](#) on page 758
  - [“\(ipv6 access-list named protocol filter\)”](#) on page 761
  - [“\(ipv6 access-list named TCP UDP filter\)”](#) on page 765
  - [“ipv6 traffic-filter”](#) on page 768
  - [“show ipv6 access-list \(IPv6 Hardware ACLs\)”](#) on page 769

## commit (IPv6)

**Overview** Use this command to commit the IPv6 ACL filter configuration entered at the console to the hardware immediately without exiting the IPv6 Hardware ACL Configuration mode.

This command forces the associated hardware and software IPv6 ACLs to synchronize.

**Syntax** `commit`

**Mode** IPv6 Hardware ACL Configuration

**Usage** Normally, when an IPv6 hardware ACL is edited, the new configuration state of the IPv6 ACL is not written to hardware until you exit IPv6 Hardware ACL Configuration mode. By entering this command you can ensure that the current state of a hardware access-list that is being edited is written to hardware immediately.

Scripts typically do not include the `exit` command to exit configuration modes, potentially leading to IPv6 ACL filters in hardware not being correctly updated. Using this **commit** command in a configuration script after specifying an IPv6 hardware ACL filter ensures that it is updated in the hardware.

**Example** To update the hardware with the IPv6 ACL filter configuration, use the command:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-ipv6-acl
awplus(config-ipv6-hw-acl)# commit
```

**Related Commands** [ipv6 access-list \(named\)](#)

## ipv6 access-list (named)

**Overview** Use this command to either create a new IPv6 hardware access-list, or to select an existing IPv6 hardware access-list in order to apply a filter entry to it.

IPv6 Hardware ACLs are supported in Software Version 5.4.3A-1.x and later.

Use the **no** variant of this command to delete an existing IPv6 hardware access-list.

**NOTE:** Before you can delete an access-list, you must first remove it from any interface it is assigned to.

**Syntax** `ipv6 access-list <ipv6-access-list-name>`  
`no ipv6 access-list <ipv6-access-list-name>`

| Parameter                                  | Description                       |
|--------------------------------------------|-----------------------------------|
| <code>&lt;ipv6-access-list-name&gt;</code> | Specify an IPv6 access-list name. |

**Mode** Global Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

**Usage** Use IPv6 hardware named access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 hardware named access-list when a match is encountered.

For backwards compatibility you can either create IPv6 hardware named access-lists from within this command, or you can enter `ipv6 access-list` followed by only the IPv6 hardware named access-list name. This latter (and preferred) method moves you to the `(config-ipv6-hw-acl)` prompt for the selected IPv6 hardware named access-list number, and from here you can configure the filters for this selected IPv6 hardware named access-list.

**NOTE:** Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples** To create an IPv6 access-list named `my-ipv6-acl`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-ipv6-acl
awplus(config-ipv6-hw-acl)#
```

To delete the IPv6 access-list named `my-ipv6-acl`, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 access-list my-ipv6-acl
```

**Validation Commands** `show ipv6 access-list (IPv6 Hardware ACLs)`

**Related  
Commands**

- (ipv6 access-list named ICMP filter)
- (ipv6 access-list named protocol filter)
- (ipv6 access-list named TCP UDP filter)
- ipv6 traffic-filter
- show ipv6 access-list (IPv6 Hardware ACLs)

## (ipv6 access-list named ICMP filter)

**Overview** Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with ICMP (Internet Control Message Protocol) packets, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Note that specifying the **send-to-cpu** parameter could result in EPSR healthcheck messages and other control packets being dropped.

As an optional parameter **vlan** can be matched for tagged (802.1q) packet.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with ICMP (Internet Control Message Protocol) packets, from the current named IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

**NOTE:** Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Syntax [ip|icmp]** [*<sequence-number>*]{deny|permit|send-to-cpu} {ipv6|icmp}  
{<ipv6-source-address/prefix-length>|<ipv6-source-address>  
<ipv6-source-wildcard>|host <ipv6-source-host>|any}  
{<ipv6-destination-address/prefix-length>|<ipv6-destination-a  
ddr> <ipv6-destination-wildcard>|host  
<ipv6-destination-host-address>|any} [<icmp-type>][vlan  
<1-4094>]  
  
no [*<sequence-number>*]{deny|permit|send-to-cpu}  
{ip|icmp}{<ipv6-source-address/prefix-length>|<ipv6-source-add  
ress> <ipv6-source-wildcard>|host <ipv6-source-host>|any}  
{<ipv6-destination-address/prefix-length>|<ipv6-destination-ad  
dress> <ipv6-destination-wildcard>|host  
<ipv6-destination-host-address>|any} [<icmp-type>][vlan  
<1-4094>]  
  
no [*<sequence-number>*]

| Parameter         | Description                                                                                                                                            |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <sequence-number> | <1-65535>The sequence number for the filter entry of the selected access control list.                                                                 |
| deny              | Specifies the packets to reject.                                                                                                                       |
| permit            | Specifies the packets to permit.                                                                                                                       |
| send-to-cpu       | Specifies the packets to send to the CPU. Specifying this parameter could result in EPSR healthcheck messages and other control packets being dropped. |
| ipv6              | IPv6 packet, defined by the following parameters.                                                                                                      |

| Parameter                                                   | Description                                                                                                                                                                            |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>icmp</code>                                           | ICMP packet, defined by the following parameters.                                                                                                                                      |
| <code>&lt;ipv6-source-address/prefix-length&gt;</code>      | Specifies a source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.                          |
| <code>&lt;ipv6-source-address&gt;</code>                    | Specifies the IPv6 source address. The IPv6 address uses the format X:X::X:X.                                                                                                          |
| <code>&lt;ipv6-source-wildcard&gt;</code>                   | Specifies source wildcard bits in IPv6 format X:X::X:X.<br>Note that binary 1 represents a don't care condition, and binary 0 represents a match.                                      |
| <code>host &lt;ipv6-source-host&gt;</code>                  | Specifies a single source host address. The IPv6 address uses the format X:X::X:X.                                                                                                     |
| <code>any</code>                                            | Specifies any Source host.                                                                                                                                                             |
| <code>&lt;ipv6-destination-address/prefix-length&gt;</code> | Specifies a destination address and prefix length. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.                         |
| <code>&lt;ipv6-destination-address&gt;</code>               | Specifies a destination address. The IPv6 address uses the format X:X::X:X.                                                                                                            |
| <code>&lt;ipv6-destination-wildcard&gt;</code>              | Specify destination wildcard bits in IPv6 format X:X::X:X.                                                                                                                             |
| <code>host &lt;ipv6-destination-host-address&gt;</code>     | Specify a single destination host address. The IPv6 address uses the format X:X::X:X.                                                                                                  |
| <code>any</code>                                            | Specifies any destination host.                                                                                                                                                        |
| <code>&lt;icmp-type&gt;</code>                              | Optional. Specify to filter by ICMP message type number. Valid values are from 0 to 255.                                                                                               |
| <code>vlan</code>                                           | This parameter can be used in either single or double-tagged VLAN networks. It is the conventional VLAN tag (VID). In a double-tagged network it is sometimes referred to as the STAG. |
| <code>&lt;1-4094&gt;</code>                                 | The VLAN VID.                                                                                                                                                                          |

**Mode** IPv6 Hardware ACL Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicate match a filter is permitted.

**Examples** To specify a hardware IPv6 access-list named `my - acl1` and add an ACL filter entry that blocks all ICMP6 echo requests, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl1
awplus(config-ipv6-hw-acl)# deny icmp any any icmp-type 128
```

To specify a hardware IPv6 access-list named `my - acl2` and add an ACL filter entry that blocks all ICMP6 echo requests on the default VLAN (`vlan1`), enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl2
awplus(config-ipv6-hw-acl)# deny icmp any any icmp-type 128
vlan 1
```

To remove an ACL filter entry that blocks all ICMP6 echo requests from the hardware IPv6 access-list named `my - acl1`, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl1
awplus(config-ipv6-hw-acl)# no deny icmp any any icmp-type 128
```

**Validation Commands** [show ipv6 access-list \(IPv6 Hardware ACLs\)](#)

**Related Commands** [ipv6 access-list \(named\)](#)  
[\(ipv6 access-list named protocol filter\)](#)  
[\(ipv6 access-list named TCP UDP filter\)](#)  
[ipv6 traffic-filter](#)  
[show ipv6 access-list \(IPv6 Hardware ACLs\)](#)



## (ipv6 access-list named protocol filter)

**Overview** Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with an IP protocol type specified, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Note that specifying the **send-to-cpu** parameter could result in EPSR healthcheck messages and other control packets being dropped.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with an IP protocol type specified, from the current named IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

**Syntax** [*<sequence-number>*] {deny|permit|send-to-cpu} {ipv6|proto  
<i>ip-protocol</i>}<br>{<i>ipv6-source-prefix/prefix-length</i>|<i>ipv6-source-address</i><br><i>ipv6-source-wildcard</i>|host <i>ipv6-source-host</i>|any}<br>{<i>ipv6-destination-prefix/prefix-length</i>|<i>ipv6-destination-add<br>ress</i> <i>ipv6-destination-wildcard</i>|host<br><i>ipv6-destination-host</i>|any}<br>[<i>sequence-number</i>]no {deny|permit|send-to-cpu} {ipv6|proto<br><i>ip-protocol</i>}<br>{<i>ipv6-source-prefix/prefix-length</i>|<i>ipv6-source-address</i><br><i>ipv6-source-wildcard</i>|host <i>ipv6-source-host</i>|any}<br>{<i>ipv6-destination-prefix/prefix-length</i>|<i>ipv6-destination-add<br>ress</i> <i>ipv6-destination-wildcard</i>|host<br><i>ipv6-destination-host</i>|any}<br>no [<i>sequence-number</i>]

| Parameter                | Description                                                                                                                                        |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| <sequence-number>        | <1-65535>The sequence number for the filter entry of the selected access control list.                                                             |
| deny                     | Specifies packets to reject.                                                                                                                       |
| permit                   | Specifies packets to permit.                                                                                                                       |
| send-to-cpu              | Specifies packets to send to the CPU. Specifying this parameter could result in EPSR healthcheck messages and other control packets being dropped. |
| ipv6                     | Specifies IPv6 packet.                                                                                                                             |
| proto <i>ip-protocol</i> | Specify IP protocol number <1-255>.                                                                                                                |

| Parameter     | Description                                                                                                                                                                                |                                                        |
|---------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------|
| <ip-protocol> | The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority <a href="http://www.iana.org/assignments/protocol-numbers">www.iana.org/assignments/protocol-numbers</a> ) |                                                        |
|               | Protocol Number                                                                                                                                                                            | Protocol Description [RFC Reference]                   |
|               | 1                                                                                                                                                                                          | Internet Control Message [RFC792]                      |
|               | 2                                                                                                                                                                                          | Internet Group Management [RFC1112]                    |
|               | 3                                                                                                                                                                                          | Gateway-to-Gateway [RFC823]                            |
|               | 4                                                                                                                                                                                          | IP in IP [RFC2003]                                     |
|               | 5                                                                                                                                                                                          | Stream [RFC1190] [RFC1819]                             |
|               | 6                                                                                                                                                                                          | TCP (Transmission Control Protocol) [RFC793]           |
|               | 8                                                                                                                                                                                          | EGP (Exterior Gateway Protocol) [RFC888]               |
|               | 9                                                                                                                                                                                          | IGP (Interior Gateway Protocol) [IANA]                 |
|               | 11                                                                                                                                                                                         | Network Voice Protocol [RFC741]                        |
|               | 17                                                                                                                                                                                         | UDP (User Datagram Protocol) [RFC768]                  |
|               | 20                                                                                                                                                                                         | Host monitoring [RFC869]                               |
|               | 27                                                                                                                                                                                         | RDP (Reliable Data Protocol) [RFC908]                  |
|               | 28                                                                                                                                                                                         | IRTP (Internet Reliable Transaction Protocol) [RFC938] |
|               | 29                                                                                                                                                                                         | ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]      |
|               | 30                                                                                                                                                                                         | Bulk Data Transfer Protocol [RFC969]                   |
|               | 33                                                                                                                                                                                         | DCCP (Datagram Congestion Control Protocol) [RFC4340]  |
|               | 48                                                                                                                                                                                         | DSR (Dynamic Source Routing Protocol) [RFC4728]        |
|               | 50                                                                                                                                                                                         | ESP (Encap Security Payload) [RFC2406]                 |
|               | 51                                                                                                                                                                                         | AH (Authentication Header) [RFC2402]                   |
|               | 54                                                                                                                                                                                         | NARP (NBMA Address Resolution Protocol) [RFC1735]      |
|               | 58                                                                                                                                                                                         | ICMP for IPv6 [RFC1883]                                |
|               | 59                                                                                                                                                                                         | No Next Header for IPv6 [RFC1883]                      |
|               | 60                                                                                                                                                                                         | Destination Options for IPv6 [RFC1883]                 |
|               | 88                                                                                                                                                                                         | EIGRP (Enhanced Interior Gateway Routing Protocol)     |
|               | 89                                                                                                                                                                                         | OSPFv2 [RFC1583]                                       |

| Parameter                              | Description                                                                                                                                                                            |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ip-protocol>(cont.)                   | 97 Ethernet-within-IP Encapsulation / RFC3378                                                                                                                                          |
|                                        | 98 Encapsulation Header / RFC1241                                                                                                                                                      |
|                                        | 108 IP Payload Compression Protocol / RFC2393                                                                                                                                          |
|                                        | 112 Virtual Router Redundancy Protocol / RFC3768                                                                                                                                       |
|                                        | 134 RSVP-E2E-IGNORE / RFC3175                                                                                                                                                          |
|                                        | 135 Mobility Header / RFC3775                                                                                                                                                          |
|                                        | 136 UDPLite / RFC3828                                                                                                                                                                  |
|                                        | 137 MPLS-in-IP / RFC4023                                                                                                                                                               |
|                                        | 138 MANET Protocols / RFC-ietf-manet-iana-07.txt                                                                                                                                       |
|                                        | 139 - 252 Unassigned / IANA                                                                                                                                                            |
|                                        | 253 Use for experimentation and testing / RFC3692                                                                                                                                      |
|                                        | 254 Use for experimentation and testing / RFC3692                                                                                                                                      |
|                                        | 255 Reserved / IANA                                                                                                                                                                    |
| <ipv6-source-prefix/<br>prefix-length> | Specify source address and mask.<br>The IPv6 address uses the format X:X::X:Prefix-Length. The prefix-length is usually set between 0 and 64.                                          |
| <ipv6-source-address>                  | Specifies the source address.<br>The IPv6 address uses the format X:X::X:X.                                                                                                            |
| <ipv6-source-wildcard>                 | Specifies the source wildcard bits, in IPv6 format X:X::X:X.                                                                                                                           |
| host <ipv6-source-host>                | Specifies a single source host.<br>The IPv6 address uses the format X:X::X:X.                                                                                                          |
| any                                    | Specifies any source host.<br>An abbreviation for the IPv6 prefix ::/0                                                                                                                 |
| <ipv6-dest-prefix/prefix-length>       | Specifies a destination address and mask.<br>The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.                           |
| <ipv6-destination-address>             | Specify destination address.<br>The IPv6 address uses the format X:X::X:X.                                                                                                             |
| <ipv6-destination-wildcard>            | Specify destination wildcard bits in IPv6 format X:X::X:X                                                                                                                              |
| host <ipv6-destination-host>           | Specify a single destination host address.<br>The IPv6 address uses the format X:X::X:X.                                                                                               |
| any                                    | Specifies any destination host. An abbreviation for the IPv6 prefix ::/0                                                                                                               |
| vlan                                   | This parameter can be used in either single or double-tagged VLAN networks. It is the conventional VLAN tag (VID). In a double-tagged network it is sometimes referred to as the STAG. |
| <1-4094>                               | The VLAN VID.                                                                                                                                                                          |

**Mode** IPv6 Hardware ACL Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicate match a filter is permitted.

**Usage** This command adds a hardware classification filter (for use with features such as QoS), to a current standard IPv6 access-list. The filter will match on any IP protocol type packet that has the specified source and destination IPv6 addresses and the specified IP protocol type. The parameter any may be specified if an address does not matter,

**NOTE:** Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples** To add an ACL filter entry to block IP traffic from network 2001:0db8::0/64 to the hardware IPv6 access-list named my-acl, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny ipv6 2001:0db8::0/64
```

To remove an ACL filter entry that blocks all IPv6 traffic from network 2001:0db8::0/64 from the hardware IPv6 access-list named my-acl, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# no deny ipv6 2001:0db8::0/64
```

**Validation Commands** show ipv6 access-list (IPv6 Hardware ACLs)

**Related Commands** ipv6 access-list (named)  
(ipv6 access-list named ICMP filter)  
(ipv6 access-list named TCP UDP filter)  
ipv6 traffic-filter  
show ipv6 access-list (IPv6 Hardware ACLs)

## (ipv6 access-list named TCP UDP filter)

**Overview** Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) source and destination ports specified, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Note that specifying the **send-to-cpu** parameter could result in EPSR healthcheck messages and other control packets being dropped.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with TCP or UDP source and destination ports specified, from the current named IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

**Syntax** [*<sequence-number>*]{deny|permit|send-to-cpu} {tcp|udp}  
{<ipv6-source-prefix/prefix-length>|<ipv6-source-address>  
<ipv6-source-wildcard>|host <ipv6-source-host>|any} eq  
<sourceport>  
{<ipv6-destination-prefix/prefix-length>|<ipv6-destination-add  
ress> <ipv6-destination-wildcard>|host  
<ipv6-destination-host>|any} eq <destport>  
  
no {deny|permit|send-to-cpu} {tcp|udp}  
{<ipv6-source-prefix/prefix-length>|<ipv6-source-address>  
<ipv6-source-wildcard>|host <ipv6-source-host>|any} eq  
<sourceport>  
{<ipv6-destination-prefix/prefix-length>|<ipv6-destination-add  
ress> <ipv6-destination-wildcard>|host  
<ipv6-destination-host>|any} eq <destport>  
  
no <sequence-number>

| Parameter                              | Description                                                                                                                                             |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <sequence-number>                      | <1-65535>The sequence number for the filter entry of the selected access control list.                                                                  |
| deny                                   | Specify packets to reject.                                                                                                                              |
| permit                                 | Specifies the packets to permit.                                                                                                                        |
| send-to-cpu                            | Specifies the packets to send to the CPU. Specifying this parameter could result in EPSR healthcheck messages and other control packets being dropped.  |
| tcp                                    | Specifies a TCP packet.                                                                                                                                 |
| udp                                    | Specifies a UDP packet.                                                                                                                                 |
| <ipv6-source-prefix/<br>prefix-length> | Specifies the source address with mask. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64. |

| Parameter                            | Description                                                                                                                                            |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipv6-source-address>                | Specifies the source address. The IPv6 address uses the format X:X::X:X.                                                                               |
| <ipv6-source-wildcard>               | Specifies the source wildcard bits in IPv6 format X:X::X:X.                                                                                            |
| host <ipv6-source-host>              | Specifies the a single source host. The IPv6 address uses the format X:X::X:X.                                                                         |
| any                                  | Specifies any Source host. An abbreviation for the IPv6 prefix ::/0.                                                                                   |
| eq                                   | Equal to.                                                                                                                                              |
| <sourceport>                         | The source port number, specified as an integer between 0 and 65535.                                                                                   |
| <destport>                           | The destination port number, specified as an integer between 0 and 65535.                                                                              |
| <ipv6-dest-prefix/<br>prefix-length> | Specify destination address with mask. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64. |
| <ipv6-destination-address>           | Specify destination address. The IPv6 address uses the format X:X::X:X.                                                                                |
| <ipv6-destination-wildcard>          | Specify destination wildcard bits in IPv6 format X:X::X:X.                                                                                             |
| host<br><ipv6-destination-host>      | Specify a single destination host address. The IPv6 address uses the format X:X::X:X.                                                                  |
| any                                  | Specifies any destination host. An abbreviation for the IPv6 prefix ::/0.                                                                              |

**Mode** IPv6 Hardware ACL Configuration

**Default** Any traffic on an interface controlled by a hardware ACL that does not explicate match a filter is permitted.

**Usage** The filter entry will match on any TCP or UDP packet that has the specified source and destination IPv6 addresses and TCP or UDP type. The parameter any may be specified if an address does not matter.

**NOTE:** Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.

**Examples** To add an ACL filter entry that blocks all SSH traffic from network 2001:0db8::0/64 to the hardware IPv6 access-list named my - ac l, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny tcp 2001:0db8::0/64 any eq 22
```

To add an ACL filter entry that blocks all SSH traffic from network 2001:0db8::0/64 on the default VLAN (v lan1) to the hardware IPv6 access-list named my - ac l, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny tcp 2001:0db8::0/64 any eq 22
vlan 1
```

To remove an ACL filter entry that blocks all SSH traffic from network 2001:0db8::0/64 from the hardware IPv6 access-list named my - ac l, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# no deny tcp 2001:0db8::0/64 any eq
22
```

**Validation Commands**    [show ipv6 access-list \(IPv6 Hardware ACLs\)](#)

**Related Commands**    [ipv6 access-list \(named\)](#)  
                          [\(ipv6 access-list named ICMP filter\)](#)  
                          [\(ipv6 access-list named protocol filter\)](#)  
                          [ipv6 traffic-filter](#)  
                          [show ipv6 access-list \(IPv6 Hardware ACLs\)](#)

# ipv6 traffic-filter

**Overview** This command adds an IPv6 hardware-based access-list to an interface. The number of access-lists that can be added is determined by the amount of available space in the hardware-based packet classification tables.

Use the **no** variant of this command to remove an IPv6 hardware-based access-list from an interface.

**Syntax** `ipv6 traffic-filter <ipv6-access-list-name>`  
`no ipv6 traffic-filter <ipv6-access-list-name>`

| Parameter                                  | Description                     |
|--------------------------------------------|---------------------------------|
| <code>&lt;ipv6-access-list-name&gt;</code> | Hardware IPv6 access-list name. |

**Mode** Interface Configuration (to apply an IPv6 hardware ACL to a specific switch port).

**Usage** This command adds an IPv6 hardware-based access-list to an interface. The number of access-lists that can be added is determined by the amount of available space in the hardware-based packet classification tables.

To apply the access-list to all ports on the switch, execute the command in the Global Configuration mode. To apply the access-list to a Layer 2 interface or Layer 2 interface range, apply the command in the Interface Configuration mode. See the examples for each mode below.

**Examples** To add access-list `acl1` as a traffic-filter to interface `port1.0.1`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# ipv6 traffic-filter acl1
```

**Related Commands**

- [ipv6 access-list \(named\)](#)
- [\(ipv6 access-list named ICMP filter\)](#)
- [\(ipv6 access-list named protocol filter\)](#)
- [\(ipv6 access-list named TCP UDP filter\)](#)
- [ipv6 traffic-filter](#)
- [show ipv6 access-list \(IPv6 Hardware ACLs\)](#)



# show ipv6 access-list (IPv6 Hardware ACLs)

**Overview** Use this command to display all configured hardware IPv6 access-lists or the IPv6 access-list specified by name. Omitting the optional access-list name parameter will display all IPv6 ACLs.

Use the **show ipv6 access-list standard** command to display the IPv6 access-list specified by name as defined from the [ipv6 access-list \(named\)](#) command.

**Syntax** `show ipv6 access-list [<access-list-name>]`  
`show ipv6 access-list standard [<access-list-name>]`

| Parameter          | Description                     |
|--------------------|---------------------------------|
| standard           | Named standard access-list.     |
| <access-list-name> | Hardware IPv6 access-list name. |

**Mode** User Exec and Privileged Exec

**Examples** To show the standard named ipv6 access-list `acl_name` use the following command:

```
awplus# show ipv6 access-list standard acl_name
```

**Output** Figure 24-1: Example output from the **show ipv6 access-list standard** command

```
Named Standard IPv6 access-list acl_name
deny any
```

To show all configured ipv6 access-lists use the command:

```
awplus# show ipv6 access-list
```

**Output** Figure 24-2: Example output from the **show ipv6 access-list** command

```
IPv6 access-list deny_icmp
deny icmp any any vlan 1

IPv6 access-list deny_ssh
deny tcp abcd::0/64 any eq 22
```

**Related  
Commands**    [ipv6 access-list \(named\)](#)  
                  [\(ipv6 access-list named ICMP filter\)](#)  
                  [\(ipv6 access-list named protocol filter\)](#)  
                  [\(ipv6 access-list named TCP UDP filter\)](#)  
                  [ipv6 traffic-filter](#)

# 25

# IPv6 Software Access Control List (ACL) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for the IPv6 Software Access Control List (ACL) commands, and contains detailed command information and command examples about IPv6 software ACLs as applied to Routing and Multicasting, which are not applied to interfaces.

For information about ACLs, see the [ACL Feature Overview and Configuration Guide](#).

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- the [Link Aggregation Feature Overview and Configuration Guide](#).
- [Link Aggregation Commands](#)

Note that text in parenthesis in command names indicates usage not keyword entry. For example, **ipv6-access-list (named)** indicates named IPv6 ACLs entered as `ipv6-access-list <name>` where *<name>* is a placeholder not a keyword.

Note also that parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI. For example, **(ipv6 access-list standard IPv6 filter)** represents command entry in the format:

[<sequence-number>] {deny|permit} {<IPv6-source-address/prefix-length>|any}.

**NOTE:** Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Sub-modes** Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 25-1: IPv6 Software Access List Commands and Prompts

| Command Name                                               | Command Mode                    | Prompt                       |
|------------------------------------------------------------|---------------------------------|------------------------------|
| <a href="#">show ipv6 access-list (IPv6 Software ACLs)</a> | Privileged Exec                 | awplus#                      |
| <a href="#">ipv6 access-list standard (named)</a>          | Global Configuration            | awplus(config)#              |
| <a href="#">(ipv6 access-list standard filter)</a>         | IPv6 Standard ACL Configuration | awplus(config-ipv6-std-acl)# |

- Command List**
- [“ipv6 access-list standard \(named\)”](#) on page 773
  - [“\(ipv6 access-list standard filter\)”](#) on page 775
  - [“show ipv6 access-list \(IPv6 Software ACLs\)”](#) on page 777

## ipv6 access-list standard (named)

**Overview** This command configures an IPv6 standard access-list for filtering frames that permit or deny IPv6 packets from a specific source IPv6 address.

The **no** variant of this command removes a specified IPv6 standard access-list.

**Syntax** **[list-name]** `ipv6 access-list standard <ipv6-acl-list-name>`  
`no ipv6 access-list standard <ipv6-acl-list-name>`

| Parameter                               | Description                                                     |
|-----------------------------------------|-----------------------------------------------------------------|
| <code>&lt;ipv6-acl-list-name&gt;</code> | A user-defined name for the IPv6 software standard access-list. |

**Syntax [deny|permit]** `ipv6 access-list standard <ipv6-acl-list-name> [{deny|permit} {<ipv6-source-address/prefix-length>|any} [exact-match]]`  
`no ipv6 access-list standard <ipv6-acl-list-name> [{deny|permit} {<ipv6-source-address/prefix-length>|any} [exact-match]]`

| Parameter                                              | Description                                                                                                                                                   |
|--------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipv6-acl-list-name&gt;</code>                | A user-defined name for the IPv6 software standard access-list.                                                                                               |
| deny                                                   | The IPv6 software standard access-list rejects packets that match the type, source, and destination filtering specified with this command.                    |
| permit                                                 | The IPv6 software standard access-list permits packets that match the type, source, and destination filtering specified with this command.                    |
| <code>&lt;ipv6-source-address/prefix-length&gt;</code> | Specifies a source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64. |
| any                                                    | Matches any source IPv6 address.                                                                                                                              |
| exact-match                                            | Exact match of the prefixes.                                                                                                                                  |

**Mode** Global Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** Use IPv6 standard access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 standard access-list when a match is encountered.

For backwards compatibility you can either create IPv6 standard access-lists from within this command, or you can enter `ipv6 access-list standard` followed by only the IPv6 standard access-list name. This latter (and preferred) method moves you to the `(config-ipv6-std-acl)` prompt for the selected IPv6 standard access-list, and from here you can configure the filters for this selected IPv6 standard access-list.

**NOTE:** Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Example** To enter the IPv6 Standard ACL Configuration mode for the access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)#
```

**Related Commands** [\(ipv6 access-list standard filter\)](#)  
[show ipv6 access-list \(IPv6 Software ACLs\)](#)  
[show running-config](#)

## (ipv6 access-list standard filter)

**Overview** Use this ACL filter to add a filter entry for an IPv6 source address and prefix length to the current standard IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a filter entry for an IPv6 source address and prefix from the current standard IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

**Syntax [icmp]** [*<sequence-number>*] {deny|permit}  
{*<ipv6-source-address/prefix-length>*|any}  
no {deny|permit} {*<ipv6-source-address/prefix-length>*|any}  
no *<sequence-number>*

| Parameter                                        | Description                                                                                             |
|--------------------------------------------------|---------------------------------------------------------------------------------------------------------|
| <i>&lt;sequence-number&gt;</i>                   | <i>&lt;1-65535&gt;</i><br>The sequence number for the filter entry of the selected access control list. |
| deny                                             | Specifies the packets to reject.                                                                        |
| permit                                           | Specifies the packets to accept.                                                                        |
| <i>&lt;ipv6-source-address/prefix-length&gt;</i> | IPv6 source address and prefix-length in the form X:X::X:X/P.                                           |
| any                                              | Any IPv6 source host address.                                                                           |

**Mode** IPv6 Standard ACL Configuration

**Default** Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

**Usage** The filter entry will match on any IPv6 packet that has the specified IPv6 source address and prefix length. The parameter any may be specified if an address does not matter.

**NOTE:** Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

**Examples** To add an ACL filter entry with sequence number 5 that will deny any IPv6 packets to the standard IPv6 access-list named my-list, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# 5 deny any
```

To remove the ACL filter entry that will deny any IPv6 packets from the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# no deny any
```

Alternately, to remove the ACL filter entry with sequence number 5 to the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# no 5
```

**Related  
Commands**

[ipv6 access-list standard \(named\)](#)  
[show ipv6 access-list \(IPv6 Software ACLs\)](#)  
[show running-config](#)



# show ipv6 access-list (IPv6 Software ACLs)

**Overview** Use the **show ipv6 access-list standard** command to display a specified standard named IPv6 access-list that has been defined using the [ipv6 access-list standard \(named\)](#) command.

**Syntax** `show ipv6 access-list standard <access-list-name>`

| Parameter          | Description                       |
|--------------------|-----------------------------------|
| standard           | Named standard access-list.       |
| <access-list-name> | Specify an IPv6 access-list name. |

**Mode** User Exec and Privileged Exec

**Example** To show the ipv6 access-list specified with the name `acl_name` use the following command:

```
awplus# show ipv6 access-list standard acl_name
```

**Output** Figure 25-1: Example output from the **show ipv6 access-list standard** command

```
Named Standard IPv6 access-list name
deny any
```

**Related Commands** [ipv6 access-list standard \(named\)](#)  
[\(ipv6 access-list standard filter\)](#)

# 26

# QoS Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for Quality of Service commands. For more information, see the [QoS Feature Overview and Configuration Guide](#) and the [ACL Feature Overview and Configuration Guide](#).

- Command List**
- ["class"](#) on page 780
  - ["class-map"](#) on page 781
  - ["default-action"](#) on page 782
  - ["description \(QoS policy-map\)"](#) on page 783
  - ["egress-rate-limit"](#) on page 784
  - ["match access-group"](#) on page 785
  - ["match cos"](#) on page 787
  - ["match dscp"](#) on page 788
  - ["match eth-format protocol"](#) on page 789
  - ["match mac-type"](#) on page 792
  - ["match tcp-flags"](#) on page 793
  - ["match vlan"](#) on page 794
  - ["mls qos cos"](#) on page 795
  - ["mls qos cpu-queue rx-rate-limit"](#) on page 796
  - ["mls qos enable"](#) on page 797
  - ["mls qos map cos-queue to"](#) on page 798
  - ["mls qos map premark-dscp to"](#) on page 799
  - ["no police"](#) on page 800
  - ["police single-rate action"](#) on page 801

- [“policy-map”](#) on page 802
- [“priority-queue”](#) on page 803
- [“remark new-cos”](#) on page 804
- [“service-policy input”](#) on page 805
- [“show class-map”](#) on page 806
- [“show mls qos”](#) on page 807
- [“show mls qos interface”](#) on page 808
- [“show mls qos maps cos-queue”](#) on page 810
- [“show policy-map”](#) on page 811
- [“trust dscp”](#) on page 812
- [“wrr-queue weight queues”](#) on page 813

# class

**Overview** Use this command to associate an existing class-map to a policy or policy-map (traffic classification), and to enter Policy Map Class Configuration mode to configure the class-map.

Use the **no** variant of this command to delete an existing class-map.

For more information on class-maps and policy-maps, see the [QoS Feature Overview and Configuration Guide](#).

If your class-map does not exist, you can create it by using the [class-map](#) command.

**Syntax** `class {<name>|default}`  
`no class <name>`

| Parameter | Description                               |
|-----------|-------------------------------------------|
| <name>    | Name of the (already existing) class-map. |
| default   | Specify the default class-map.            |

**Mode** Policy Map Configuration

**Example** The following example creates the policy-map pmap1 (using the policy-map command), then associates this to an already existing class-map named cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)#
```

**Related Commands** [class-map](#)  
[policy-map](#)

# class-map

**Overview** Use this command to create a class-map.  
Use the **no** variant of this command to delete the named class-map.

**Syntax** class-map <name>  
no class-map <name>

| Parameter | Description                          |
|-----------|--------------------------------------|
| <name>    | Name of the class-map to be created. |

**Mode** Global Configuration

**Example** This example creates a class-map called cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)#
```

# default-action

**Overview** Sets the action for the default class-map belonging to a particular policy-map. The action for a non-default class-map depends on the action of any ACL that is applied to the policy-map.

The default action can therefore be thought of as specifying the action that will be applied to any data that does not meet the criteria specified by the applied matching commands.

Use the **no** variant of this command to reset to the default action of 'permit'.

**Syntax** `default-action [permit|deny|send-to-cpu]`  
`no default-action`

| Parameter   | Description                         |
|-------------|-------------------------------------|
| permit      | Packets to permit.                  |
| deny        | Packets to deny.                    |
| send-to-cpu | Specify packets to send to the CPU. |

**Default** The default is 'permit'.

**Mode** Policy Map Configuration

**Examples** To set the action for the default class-map to deny, use the command:  
`awplus(config-pmap)# default-action deny`

## description (QoS policy-map)

**Overview** Adds a textual description of the policy-map. This can be up to 80 characters long. Use the **no** variant of this command to remove the current description from the policy-map.

**Syntax** `description <line>`  
`no description`

| Parameter                 | Description                               |
|---------------------------|-------------------------------------------|
| <code>&lt;line&gt;</code> | Up to 80 character long line description. |

**Mode** Policy Map Configuration

**Example** To add the description, VOIP traffic, use the command:  
`awplus(config-pmap)# description VOIP traffic`

# egress-rate-limit

**Overview** Sets a limit on the amount of traffic that can be transmitted per second from this port.

Use the **no** variant of this command to disable the limiting of traffic egressing on the interface.

**Syntax** egress-rate-limit <bandwidth>  
no egress-rate-limit

| Parameter   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <bandwidth> | Bandwidth <1-10000000 units per second> (usable units: k, m, g). The egress rate limit can be configured in multiples of 64kbps. If you configure a value that is not an exact multiple of 64kbps, then the value will be rounded up to the nearest higher exact multiple of 64kbps. The minimum is 64 Kb. The default unit is Kb ( <b>k</b> ), but Mb ( <b>m</b> ) or Gb ( <b>g</b> ) can also be specified. The command syntax is not case sensitive, so a value such as 20m or 20M will be taken as 20 megabits. |

**Mode** Interface Configuration

**Examples** To enable egress rate limiting on a port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# egress-rate-limit 64k
% Egress rate limit has been set to 64 Kb
```

To disable egress rate limiting on a port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no egress-rate-limit
```



# match access-group

**Overview** Use this command to define match criterion for a class-map.

**Syntax** match access-group {<hw-IP-ACL>|<hw-MAC-ACL>|<hw-named-ACL>}  
no match access-group  
{<hw-IP-ACL>|<hw-MAC-ACL>|<hw-named-ACL>}

| Parameter      | Description                                                 |
|----------------|-------------------------------------------------------------|
| <hw-IP-ACL>    | Specify a hardware IP ACL number in the range <3000-3699>.  |
| <hw-MAC-ACL>   | Specify a hardware MAC ACL number in the range <4000-4699>. |
| <hw-named-ACL> | Specify the hardware named ACL.                             |

**Mode** Class Map Configuration

**Usage** First create an access-list that applies the appropriate permit/deny requirements. Then use the **match access-group** command to apply this access-list for matching to a class-map. Note that this command will apply the access-list matching only to *incoming* data packets.

**Examples** To configure a class-map named cmap1 with one match criterion: access - list 3001, which allows IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 3001 permit ip any any
awplus(config)# class-map cmap1
awplus(config-cmap)# match access-group 3001
```

To configure a class-map named cmap2 with one match criterion: access - list 3001, which allows MAC traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 permit any any
awplus(config)# class-map cmap2
awplus(config-cmap)# match access-group 4001
```

To configure a class-map named cmap3 with one match criterion: access - list hw\_acl, which allows IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware hw_acl
awplus(config-ip-hw-acl)# permit ip any any
awplus(config)# class-map cmap3
awplus(config-cmap)# match access-group hw_acl
```

**Related  
Commands** [class-map](#)

# match cos

**Overview** Use this command to define a COS to match against incoming packets.  
Use the **no** variant of this command to remove CoS.

**Syntax** match cos <0-7>  
no match cos

| Parameter | Description            |
|-----------|------------------------|
| <0-7>     | Specify the CoS value. |

**Mode** Class Map Configuration

**Examples** To set the class-map's CoS to 4, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match cos 4
```

To remove CoS from a class-map, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match cos
```

# match dscp

**Overview** Use this command to define the DSCP to match against incoming packets.  
Use the **no** variant of this command to remove a previously defined DSCP.

**Syntax** match dscp <0-63>  
no match dscp

| Parameter | Description                                           |
|-----------|-------------------------------------------------------|
| <0-63>    | Specify DSCP value (only one value can be specified). |

**Mode** Class Map Configuration

**Usage** Use the **match dscp** command to define the match criterion after creating a class-map.

**Examples** To configure a class-map named cmap1 with criterion that matches DSCP 56, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match dscp 56
```

To remove a previously defined DSCP from a class-map named cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match dscp
```

**Related  
Commands** [class-map](#)

# match eth-format protocol

**Overview** This command sets the Ethernet format and the protocol for a class-map to match on.

Select one Layer 2 format and one Layer 3 protocol when you issue this command.

Use the **no** variant of this command to remove the configured Ethernet format and protocol from a class-map.

**Syntax** `match eth-format <layer-two-format> protocol  
<layer-three-protocol>  
no match eth-format protocol`

| Parameter                            | Description                                                                                                              |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;layer-two-formats&gt;</i>     |                                                                                                                          |
| ethii-tagged                         | EthII Tagged Packets (enter the parameter name).                                                                         |
| ethii-untagged                       | EthII Untagged Packets (enter the parameter name).                                                                       |
| ethii-any                            | EthII Tagged or Untagged Packets (enter the parameter name).                                                             |
| <i>&lt;layer-three-protocols&gt;</i> |                                                                                                                          |
| <word>                               | A Valid Protocol Number in hexadecimal.                                                                                  |
| any                                  | Note that the parameter "any" is only valid when used with the netwarerawtagged and netwarerawuntagged protocol options. |
| sna-path-control                     | Protocol Number 04 (enter the parameter name or its number).                                                             |
| proway-lan                           | Protocol Number 0E (enter the parameter name or its number).                                                             |
| eia-rs Protocol                      | Number 4E (enter the parameter name or its number).                                                                      |
| proway Protocol                      | Number 8E (enter the parameter name or its number).                                                                      |
| ipx-802dot2                          | Protocol Number E0 (enter the parameter name or its number).                                                             |
| netbeui                              | Protocol Number F0 (enter the parameter name or its number).                                                             |
| iso-clns-is                          | Protocol Number FE (enter the parameter name or its number).                                                             |
| xdot75-internet                      | Protocol Number 0801(enter the parameter name or its number).                                                            |
| nbs-internet                         | Protocol Number 0802 (enter the parameter name or its number).                                                           |
| ecma-internet                        | Protocol Number 0803 (enter the parameter name or its number).                                                           |

| Parameter         | Description                                                    |
|-------------------|----------------------------------------------------------------|
| chaosnet          | Protocol Number 0804 (enter the parameter name or its number). |
| xdot25-level-3    | Protocol Number 0805 (enter the parameter name or its number). |
| arp Protocol      | Number 0806 (enter the parameter name or its number).          |
| xns-compatible    | Protocol Number 0807 (enter the parameter name or its number). |
| banyan-systems    | Protocol Number 0BAD (enter the parameter name or its number). |
| bbn-simnet        | Protocol Number 5208 (enter the parameter name or its number). |
| dec-mop-dump-ld   | Protocol Number 6001 (enter the parameter name or its number). |
| dec-mop-rem-cdons | Protocol Number 6002 (enter the parameter name or its number). |
| dec-decnet        | Protocol Number 6003 (enter the parameter name or its number). |
| dec-lat           | Protocol Number 6004 (enter the parameter name or its number). |
| dec-diagnostic    | Protocol Number 6005 (enter the parameter name or its number). |
| dec-customer      | Protocol Number 6006 (enter the parameter name or its number). |
| dec-lavc          | Protocol Number 6007 (enter the parameter name or its number). |
| rarp              | Protocol Number 8035 (enter the parameter name or its number). |
| dec-lanbridge     | Protocol Number 8038 (enter the parameter name or its number). |
| dec-encryption    | Protocol Number 803D (enter the parameter name or its number). |
| appletalk         | Protocol Number 809B (enter the parameter name or its number). |
| ibm-sna           | Protocol Number 80D5 (enter the parameter name or its number). |
| appletalk-aarp    | Protocol Number 80F3 (enter the parameter name or its number). |
| snmp              | Protocol Number 814CV.                                         |
| ethertalk-2       | Protocol Number 809B (enter the parameter name or its number). |

| Parameter        | Description                                                    |
|------------------|----------------------------------------------------------------|
| ethertalk-2-aarp | Protocol Number 80F3 (enter the parameter name or its number). |
| ipx-snap         | Protocol Number 8137 (enter the parameter name or its number). |
| ipx-802dot3      | Protocol Number FFFF (enter the parameter name or its number). |
| ip               | Protocol Number 0800 (enter the parameter name or its number). |
| ipx              | Protocol Number 8137 (enter the parameter name or its number). |

**Mode** Class Map Configuration

**Examples** To set the eth-format to ethii-tagged and the protocol to 0800 (IP) for class-map cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match eth-format ethii-tagged protocol
0800
awplus#
awplus(config-cmap)# match eth-format ethii-tagged protocol ip
```

To remove the eth-format and the protocol from the class-map cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match eth-format protocol
```

# match mac-type

**Overview** Use this command to set the MAC type for a class-map to match on.  
Use **no** variant of this command to remove the MAC type match entry.

**Syntax** `match mac-type {l2bcast|l2mcast|l2ucast}`  
`no match mac-type`

| Parameter | Description                |
|-----------|----------------------------|
| l2bcast   | Layer 2 Broadcast traffic. |
| l2mcast   | Layer 2 Multicast traffic. |
| l2ucast   | Layer 2 Unicast traffic.   |

**Mode** Class Map Configuration

**Examples** To set the class-map's MAC type to Layer 2 multicast, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match mac-type l2mcast
```

To remove the class-map's MAC type entry, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match mac-type
```



# match tcp-flags

**Overview** Sets one or more TCP flags (control bits) for a class-map to match on.  
Use the **no** variant of this command to remove one or more TCP flags for a class-map to match on.

**Syntax** `match tcp-flags {[ack][fin][psh][rst][syn]}`  
`no match tcp-flags {[ack][fin][rst][syn]}`

| Parameter | Description  |
|-----------|--------------|
| ack       | Acknowledge. |
| fin       | Finish.      |
| psh       | Push         |
| rst       | Reset.       |
| syn       | Synchronize. |

**Mode** Class Map Configuration

**Examples** To set the class-map's TCP flags to ack and syn, use the commands:

```
awplus# configure terminal
awplus(config)# class-map
awplus(config-cmap)# match tcp-flags ack syn
```

To remove the TCP flags ack and rst, use the commands:

```
awplus# configure terminal
awplus(config)# class-map
awplus(config-cmap)# no match tcp-flags ack rst
```

# match vlan

**Overview** Use this command to define the VLAN ID as match criteria.  
Use the **no** variant of this command to disable the VLAN ID used as match criteria.

**Syntax** match vlan <1-4094>  
no match vlan

| Parameter | Description      |
|-----------|------------------|
| <1-4094>  | The VLAN number. |

**Mode** Class Map Configuration

**Examples** To configure a class-map named cmap1 to include traffic from VLAN 3, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match vlan 3
```

To disable the configured VLAN ID as a match criteria for the class-map named cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match vlan
```

# mls qos cos

**Overview** This command assigns a CoS (Class of Service) user-priority value to untagged frames entering a specified interface. By default, all untagged frames are assigned a CoS value of 0.

Use the **no** variant of this command to return the interface to the default CoS setting for untagged frames entering the interface.

**Syntax** mls qos cos <0-7>  
no mls qos cos

| Parameter | Description                                |
|-----------|--------------------------------------------|
| <0-7>     | The Class of Service, user-priority value. |

**Default** By default, all untagged frames are assigned a CoS value of 0. Note that for tagged frames, the default behavior is not to alter the CoS value.

**Mode** Interface Configuration

**Example** To assign a CoS user priority value of 2 to all untagged packets entering ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# mls qos cos 2
```

# mls qos cpu-queue rx-rate-limit

**Overview** This command is used to limit the amount of traffic received per second by a CPU queue. Limiting the traffic rate through the queues prevents the CPU from becoming overwhelmed.

Use the **no** variant of this command to remove the traffic limit rate from a queue or queues.

**Syntax** mls qos cpu-queue rx-rate-limit <1-1000000> queues <0-3>  
no mls qos cpu-queue rx-rate-limit queues <0-3>

| Parameter   | Description                                                                                         |
|-------------|-----------------------------------------------------------------------------------------------------|
| <1-1000000> | The maximum rate at which a CPU queue will accept traffic, measured in kilo bits per second (Kbps). |
| <0-3>       | The queue number(s) to be configured.                                                               |

**Default** By default the rate at which packets are received by a queue is unlimited.

**Mode** Global Configuration

**Usage** Values are rounded as shown in the following table:

| CLI Setting     | Step | Actual Rate Limit Values      | Rounding |
|-----------------|------|-------------------------------|----------|
| 1 to 1792       | 64   | 64, 128, 192, ..., 1792       | Up       |
| 1793 to 2047    |      | 1792                          | Down     |
| 2048 to 1000000 | 1024 | 2048, 3072, 4096, ..., 999424 | Down     |

**Examples** To assign a traffic rate limit of 2048 Kbps to queue 0, use the command:

```
awplus# configure terminal
awplus(config)# mls qos cpu-queue rx-rate-limit 2048 queues 0
```

**Output** Figure 26-1: Example output from the mls qos cpu-queue rx-rate-limit command

```
awplus(config)#mls qos cpu-queue rx-rate-limit 4000 queues 0
% Receive rate limit of queue 0 has been set to 3072 Kbps
```

**Related commands** [show mls qos interfacewrr-queue weight queuesegress-rate-limit](#)

# mls qos enable

**Overview** Use this command to globally enable QoS on the switch.

Use the **no** variant of this command to globally disable QoS and remove all QoS configuration. The **no** variant of this command removes all class-maps, policy-maps, and policers that have been created. Running the **no mls qos** command will therefore remove all pre-existing QoS configurations on the switch.

**Mode** Global Configuration

**Syntax** mls qos enable  
no mls qos

**Example** To enable QoS on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# mls qos enable
```

# mls qos map cos-queue to

**Overview** Use this command to set the default CoS to egress queue mapping. This is the default queue mapping for packets that do not get assigned an egress queue via any other QoS functionality.

Use the **no** variant of this command to reset the cos-queue map back to its default setting. The default mappings for this command are:

```
CoS Priority : 0 1 2 3 4 5 6 7

CoS QUEUE:
 1 0 0 1 2 2 3 3
```

**Syntax** mls qos map cos-queue <cos-priority> to <queue-number>  
no mls qos map cos-queue

| Parameter      | Description                                           |
|----------------|-------------------------------------------------------|
| <cos-priority> | CoS priority value. Can take a value between 0 and 7. |
| <queue-number> | Queue number. Can take a value between 0 and 3.       |

**Mode** Global Configuration

**Examples** To map CoS 2 to queue 0, use the command:

```
awplus# configure terminal
awplus(config)# mls qos map cos-queue 2 to 0
```

To set the cos-queue map back to its defaults, use the command:

```
awplus# configure terminal
awplus(config)# no mls qos map cos-queue
```

**Related Commands** [show mls qos interface](#)

# mls qos map premark-dscp to

**Overview** This command configures the premark-dscp map. It is used when traffic is classified by a class-map that has **trust dscp** configured. Based on a lookup DSCP, the map determines new QoS settings for the traffic.

The **no** variant of this command resets the premark-dscp map to its defaults. If no DSCP is specified then all DSCP entries will be reset to their defaults.

This command is supported in Software Version 5.4.3A-1.x and later.

**Syntax** `mls qos map premark-dscp <0-63> to [new-queue <0-4>]`  
`no mls qos map premark-dscp [<0-63>]`

| Parameter           | Description                |
|---------------------|----------------------------|
| premark-dscp <0-63> | The DSCP value on ingress. |
| new-queue <0-3>     | Modify Egress Queue.       |

**Mode** Global Configuration

**Usage** With the **trust dscp** command set, the **mls qos map premark-dscp** command enables you to specify the queue for packets.

When **trust dscp** is enabled on a port, the switch cannot use the CoS (802.1p priority) value to determine queue settings for traffic egressing that port. Therefore, non-IP packets will not be prioritized on that port. Non-IP packets will all go into queue 0.

**NOTE:**

**Example** To send packets to queue 2 if they have a DSCP of 34, use the commands:

```
awplus# configure terminal
awplus(config)# mls qos map premark-dscp 34 to new-queue 2
```

**Example** To reset the entry for DSCP 1 use the command:

```
awplus# configure terminal
awplus(config)# no mls qos map premark-dscp 1
```

# no police

**Overview** Use this command to disable any policer previously configured on the class-map.

**Syntax** no police

**Mode** Policy Map Class Configuration

**Usage** This command disables any policer previously configured on the class-map.

**Example** To disable policing on a class-map use the command:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# no police
```



# police single-rate action

**Overview** Configures a single-rate policer for a class-map.

## Syntax

```
police single-rate <rate> <number> <number> action drop-red
```

| Parameter | Description                                                                         |
|-----------|-------------------------------------------------------------------------------------|
| <rate>    | Specify the maximum rate (1-16000000 kbps).                                         |
| <number>  | Specify any decimal number between 0 and 16777216. The switch ignores these values. |
| action    | Specify the action if the rate is exceeded.                                         |
| drop-red  | Drop the red packets.                                                               |

**Mode** Policy Map Class Configuration

**Usage** You can use a policer to meter the traffic on a port and drop non-conforming (red) packets.

**Example** To configure a single rate meter measuring traffic of 10 Mbps that drops a sustained burst of traffic over this rate, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# police single-rate 10000 1875000 1875000
action drop-red
```

**Related Commands** [no police](#)

# policy-map

**Overview** Use this command to create a policy-map and to enter Policy Map Configuration mode to configure the specified policy-map.

Use the **no** variant of this command to delete an existing policy-map.

**Syntax** `policy-map <name>`  
`no policy-map <name>`

| Parameter | Description             |
|-----------|-------------------------|
| <name>    | Name of the policy-map. |

**Mode** Global Configuration

**Example** To create a policy-map called pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)#
```

**Related  
Commands** [class-map](#)

# priority-queue

**Overview** This command configures strict priority based scheduling.

**Syntax** `priority-queue 0 1 2 3`

| Parameter | Description                                                                                                                                                                                               |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 0 1 2 3   | Set the switch's queues to use strict priority scheduling. With strict priority scheduling, the switch will empty the highest numbered queue first, then start processing the next lowest numbered queue. |

**Mode** Interface Configuration.

Note that the switch applies the setting to all ports.

**Usage** Queue scheduling is a system-wide setting. All queues on all ports must use the same setting. By default, the queues on all ports are set for priority queuing.

If any queues are set to use weighted round robin, all queues use it.

This means that the switch only uses strict priority if all queues are set to use strict priority.

When you enter a command to set a WRR weight on a queue, the switch applies that to all ports. It displays the following message to indicate this:

```
awplus(config-if)#wrr-queue weight 2 queues 0
% Queue weight changed for all ports
% All egress queues set to WRR scheduling
```

Note that the emptying sequence for priority queuing is always highest queue number to lowest queue number.

**Example** To apply priority based scheduling, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# priority-queue 0 1 2 3
```

**Related Commands** [show mls qos interface](#)  
[wrr-queue weight queues](#)

# remark new-cos

**Overview** This command enables you to configure and remark the CoS flag in the data packet and the input into the CoS to queue map. This changes the destination egress queue.

**Syntax** remark new-cos <0-7> both  
no remark new-cos both

| Parameter | Description                                                                                                                                           |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| <0-7>     | The new value for the CoS flag and/or the input into the CoS to queue map.<br>The new value for the CoS flag and the input into the CoS to queue map. |
| both      | Remarks (with the same value) both the CoS flag in the packet and the input to the CoS to queue map.                                                  |

**Mode** Policy Map Class Configuration

**Usage** The default CoS to Queue mappings are shown in the following table:

|                 |   |   |   |   |   |   |   |   |
|-----------------|---|---|---|---|---|---|---|---|
| CoS Value       | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| Egress Queue No | 1 | 0 | 0 | 1 | 2 | 2 | 3 | 3 |

**Example** For policy-map pmap3 and class-map cmap1, set the CoS value to 2 and also set the input to the CoS to queue map so that the traffic is assigned to egress queue 0:

```
awplus# configure terminal
awplus(config)# policy-map pmap3
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark new-cos 2 both
```

**Related Commands** mls qos map cos-queue to  
show mls qos maps cos-queue

# service-policy input

**Overview** Use this command to apply a policy-map to the input of an interface.  
Use the **no** variant of this command to remove a policy-map and interface association.

**Syntax** service-policy input *<policy-map>*  
no service-policy input *<policy-map>*

| Parameter                 | Description                                        |
|---------------------------|----------------------------------------------------|
| <i>&lt;policy-map&gt;</i> | Policy map name that will be applied to the input. |

**Mode** Interface Configuration

**Usage** This command can be applied to switch ports or static channel groups, but not to dynamic (LACP) channel groups.

**Example** To apply a policy-map named pmap1 to interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# service-policy input pmap1
```

# show class-map

**Overview** Use this command to display the QoS class-maps' criteria for classifying traffic.

**Syntax** show class-map [*<class-map-name>*]

| Parameter                     | Description            |
|-------------------------------|------------------------|
| <i>&lt;class-map-name&gt;</i> | Name of the class-map. |

**Mode** User Exec and Privileged Exec

**Example** To display a QoS class-map's match criteria for classifying traffic, use the command:

```
awplus# show class-map cmap1
```

**Output** Figure 26-2: Example output from the **show class-map** command

```
awplus#show class-map

CLASS-MAP-NAME: myClass
Match Mac Type: 2 l2mcast

CLASS-MAP-NAME: default
```

**Related  
Commands** [class-map](#)

# show mls qos

**Overview** Use this command to display whether QoS is enabled or disabled on the switch.

**Syntax** show mls qos

**Mode** User Exec and Privileged Exec

**Example** To display whether QoS is enabled or disabled, use the command:

```
awplus# show mls qos
```

**Output** Figure 26-3: Example output from the **show mls qos** command

```
awplus#show mls qos
Enable
```

**Related  
Commands** [mls qos enable](#)

# show mls qos interface

**Overview** Displays the current settings for the interface. This includes its default CoS and queue, scheduling used for each queue, and any policies/maps that are attached.

**Syntax** `show mls qos interface [<port>]`

| Parameter | Description  |
|-----------|--------------|
| <port>    | Switch port. |

**Mode** User Exec and Privileged Exec

**Example** To display current CoS and queue settings for interface `port1.0.1`, use the command:

```
awplus# show mls qos interface port1.0.1
```



**Output** Figure 26-4: Example output from the **show mls qos interface** command

```
awplus#show mls qos interface port1.0.1
Interface: port1.0.1

INPUT-POLICY-MAP-NAME: myPolicy
 CLASS-MAP-NAME: default
 Policer counters enabled
 CLASS-MAP-NAME: myClass
 Match Mac Type: 2 l2mcast
 Policer counters enabled
 Remark CoS and CoS-Queue Map Index to 6

Number of egress queues: 4

Egress Queue: 0
 Status: Enabled
 Scheduler: Strict Priority

Egress Queue: 1
 Status: Enabled
 Scheduler: Strict Priority

Egress Queue: 2
 Status: Enabled
 Scheduler: Strict Priority

Egress Queue: 3
 Status: Enabled
 Scheduler: Strict Priority

Trust Mode: Ports default priority
VLAN Priority Override: Not Configured
Egress Traffic Shaping: Not Configured
 The number of COS Values mapped: 8
 Cos (Queue): 0(1), 1(0), 2(0), 3(1), 4(2), 5(2), 6(3), 7(3)
```

# show mls qos maps cos-queue

**Overview** Show the current configuration of the cos-queue map.

**Syntax** show mls qos maps cos-queue

**Mode** User Exec and Privileged Exec

**Example** To display the current configuration of the cos-queue map, use the command:

```
awplus# show mls qos maps cos-queue
```

**Output** Figure 26-5: Example output from the **show mls qos maps cos-queue** command

```
COS-TO-QUEUE-MAP:
COS : 0 1 2 3 4 5 6 7

QUEUE: 1 0 0 1 2 2 3 3
```

**Related Commands** [mls qos map cos-queue to](#)

# show policy-map

**Overview** Displays the policy-maps configured on the switch. The output also shows whether or not they are connected to a port (attached / detached) and shows their associated class-maps.

**Syntax** show policy-map [*<name>*]

| Parameter           | Description                        |
|---------------------|------------------------------------|
| <i>&lt;name&gt;</i> | The name of a specific policy-map. |

**Mode** User Exec and Privileged Exec

**Example** To display a listing of the policy-maps configured on the switch, use the command:

```
awplus# show policy-map
```

**Output** Figure 26-6: Example output from the **show policy-map** command

```
awplus#show policy-map

POLICY-MAP-NAME: myPolicy
 State: attached
 Default class-map action: permit

 CLASS-MAP-NAME: default
 Policer counters enabled

 CLASS-MAP-NAME: myClass
 Match Mac Type: 2 l2mcast
 Policer counters enabled
 Remark CoS and CoS-Queue Map Index to 6
```

**Related Commands** [service-policy input](#)

# trust dscp

**Overview** This command enables the premark-dscp map to send traffic to a particular egress queue, based on a lookup DSCP value.

This command is supported in Software Version 5.4.3A-1.x and later.

**Syntax** trust dscp  
no trust

**Mode** Policy-Map Configuration. Because policy-maps are applied to ports, you can think of **trust dscp** as a per-port setting.

**Examples** To enable the premark-dscp map lookup for policy-map pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# trust dscp
```

To disable the premark-dscp map lookup for policy-map pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# no trust
```

**Related Commands** [mls qos map premark-dscp to](#)

## wrr-queue weight queues

**Overview** This command configures weighted round-robin based scheduling on the specified egress queues on switch port interfaces only. The weights are specified as ratios relative to each other.

**Syntax** `wrr-queue weight <1-15> queues [0][1][2][3]`

| Parameter    | Description                                                                          |
|--------------|--------------------------------------------------------------------------------------|
| <1-15>       | Weight (the higher the number the greater will be the queue servicing).              |
| [0][1][2][3] | Enter egress queue numbers 0-3, to assign the specified queues the specified weight. |

**Mode** Interface Configuration for switch port interfaces only (not for static aggregated interfaces).

**Usage** If any queues are set to use weighted round robin, all queues use it.

When you enter a command to set a WRR weight on a queue, the switch applies that to all ports. It displays the following message to indicate this:

```
awplus(config-if)#wrr-queue weight 2 queues 0
% Queue weight changed for all ports
% All egress queues set to WRR scheduling
```

Only apply weighted round-robin based scheduling to switch port interfaces (for example, `awplus(config)#interface port1.0.2`).

You cannot apply weighted round-robin based scheduling to static aggregated interfaces (for example, `awplus(config)#interface sa2`). Attempting to apply weighted round-robin based scheduling on aggregated interfaces will display the console error shown below:

```
awplus# configure terminal
awplus(config)# interface sa2
awplus(config-if)# wrr-queue weight
% Invalid input detected at ^ marker
```

**Example** In this example, the queues are configured as follows:

- queue 3 is configured WRR with a weighting value of 15
- queue 2 is configured WRR with a weighting value of 8

- queues 0 and 1 are configured as WRR with weighting values of 4

```
awplus# configure terminal
awplus(config)# interface port1.0.1-1.0.6
awplus(config-if)# wrr-queue weight 15 queues 3
awplus(config-if)# wrr-queue weight 8 queues 2
awplus(config-if)# wrr-queue weight 4 queues 0 1
```

In this example, the queues are processed in turn. Four times as much traffic goes out queue 3 as goes out queues 0 or 1.

**Related** [priority-queue](#)  
**Commands** [show mls qos interface](#)

# 27

# 802.1X Commands

## Introduction

**Overview** This chapter provides an alphabetical reference of commands used to configure 802.1X port access control.

- Command List**
- “[debug dot1x](#)” on page 816
  - “[dot1x control-direction](#)” on page 817
  - “[dot1x eap](#)” on page 818
  - “[dot1x eapol-version](#)” on page 819
  - “[dot1x initialize interface](#)” on page 820
  - “[dot1x initialize supplicant](#)” on page 821
  - “[dot1x keytransmit](#)” on page 822
  - “[dot1x max-auth-fail](#)” on page 823
  - “[dot1x max-reauth-req](#)” on page 825
  - “[dot1x port-control](#)” on page 826
  - “[dot1x timeout tx-period](#)” on page 828
  - “[show debugging dot1x](#)” on page 829
  - “[show dot1x](#)” on page 830
  - “[show dot1x diagnostics](#)” on page 833
  - “[show dot1x interface](#)” on page 835
  - “[show dot1x sessionstatistics](#)” on page 840
  - “[show dot1x statistics interface](#)” on page 841
  - “[show dot1x supplicant](#)” on page 842
  - “[show dot1x supplicant interface](#)” on page 844
  - “[undebug dot1x](#)” on page 847

# debug dot1x

**Overview** Use this command to enable 802.1X IEEE Port-Based Network Access Control troubleshooting functions.

Use the **no** variant of this command to disable this function.

**Syntax** debug dot1x [all|auth-web|event|nsm|packet|timer]  
no debug all dot1x  
no debug dot1x [all|auth-web|event|nsm|packet|timer]

| Parameter | Description                                                                                      |
|-----------|--------------------------------------------------------------------------------------------------|
| all       | Used with the <b>no</b> variant of this command exclusively; turns off all debugging for 802.1X. |
| auth-web  | Specifies debugging for 802.1X auth-web information.                                             |
| events    | Specifies debugging for 802.1X events.                                                           |
| nsm       | Specifies debugging for NSM messages.                                                            |
| packet    | Specifies debugging for 802.1X packets.                                                          |
| timer     | Specifies debugging for 802.1X timers.                                                           |

**Mode** Privileged Exec and Global Configuration

**Usage** This command without any parameters turns on normal 802.1X debug information.

```
awplus# debug dot1x
awplus# show debugging dot1x
```

```
802.1X debugging status:

802.1X events debugging is

802.1X timer debugging is on

802.1X packets debugging is on

802.1X NSM debugging is on
```

**Examples** awplus# debug dot1x  
awplus# debug dot1x all

**Related Commands** show debugging dot1x  
undebug dot1x



# dot1x control-direction

- Overview** This command sets the direction of the filter for the unauthorized interface.
- If the optional **in** parameter is specified with this command then packets entering the specified port are discarded. The **in** parameter discards the ingress packets received from the supplicant.
- If the optional **both** parameter is specified with this command then packets entering (ingress) and leaving (egress) the specified port are discarded. The **both** parameter discards the packets received from the supplicant and sent to the supplicant.
- The **no** variant of this command sets the direction of the filter to **both**. The port will then discard both ingress and egress traffic.

**Syntax** dot1x control-direction {in|both}  
no dot1x control-direction

| Parameter | Description                                                                                                                |
|-----------|----------------------------------------------------------------------------------------------------------------------------|
| in        | Discard received packets from the supplicant (ingress packets).                                                            |
| both      | Discard received packets from the supplicant (ingress packets) and transmitted packets to the supplicant (egress packets). |

- Default** The authentication port direction is set to **both** by default.
- Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Example s** To set the port direction to the default (**both**) for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x control-direction
```

To set the port direction to **in** for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x control-direction in
```

**Validation Commands**

- show dot1x
- show dot1x interface
- show auth-mac interface
- show auth-web interface

# dot1x eap

**Overview** This command selects the transmit mode for the EAP packet. If the authentication feature is not enabled then EAP transmit mode is not enabled. The default setting discards EAP packets.

**Syntax** `dot1x eap {discard|forward|forward-untagged-vlan|forward-vlan}`

| Parameter             | Description                                   |
|-----------------------|-----------------------------------------------|
| discard               | Discard.                                      |
| forward               | Forward to all ports on the switch.           |
| forward-untagged-vlan | Forward to ports with the same untagged VLAN. |
| forward-vlan          | Forward to ports with the same VLAN.          |

**Default** The transmit mode is set to discard EAP packets by default.

**Mode** Global Configuration

**Examples** To set the transmit mode of EAP packet to forward to forward EAP packets to all ports on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward
```

To set the transmit mode of EAP packet to discard to discard EAP packets, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap discard
```

To set the transmit mode of EAP packet to forward-untagged-vlan to forward EAP packets to ports with the same untagged vlan, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward-untagged-vlan
```

To set the transmit mode of EAP packet to forward-vlan to forward EAP packets to ports with the same vlan, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward-vlan
```

# dot1x eapol-version

**Overview** This command sets the EAPOL protocol version for EAP packets when 802.1X port authentication is applied.

Use the **no** variant of this command to set the EAPOL protocol version to 1.

The default EAPOL protocol version is version 1.

**Syntax** dot1x eapol-version {1|2}  
no dot1x eapol-version

| Parameter | Description    |
|-----------|----------------|
| 1         | EAPOL version. |
| 2         | EAPOL version. |

**Default** The EAP version for 802.1X authentication is set to 1 by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To set the EAPOL protocol version to 2 for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x eapol-version 2
```

To set the EAPOL protocol version to the default version (1) for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x eapol-version
```

**Validation Commands** show dot1x  
show dot1x interface

# dot1x initialize interface

**Overview** This command removes authorization for a connected **interface** with the specified `<interface-list>`. The connection will attempt to re-authorize when the specified **port** attempts to make use of the network connection.

**NOTE:** *Reauthentication could be a long time after the use of this command because the reauthorization attempt is not triggered by this command. The attempt is triggered by the first packet from the interface trying to access the network resources.*

**Syntax** `dot1x initialize interface <interface-list>`

| Parameter                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;interface-list&gt;</code> | <p>The interfaces or ports to configure. An interface-list can be:</p> <ul style="list-style-type: none"><li>• an interface (e.g. <code>vlan2</code>), a switch port (e.g. <code>port1.0.6</code>), a static channel group (e.g. <code>sa2</code>) or a dynamic (LACP) channel group (e.g. <code>po2</code>)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. <code>vlan2-8</code>, or <code>port1.0.1-1.0.6</code>, or <code>sa1-2</code>, or <code>po1-2</code></li><li>• a comma-separated list of the above; e.g. <code>port1.0.1, port1.0.2-1.0.4</code>. Do not mix interface types in a list</li></ul> <p>The specified interfaces must exist.</p> |

**Mode** Privileged Exec

**Examples** To initialize 802.1X port authentication on the interface `port1.0.2`, use the command:

```
awplus# dot1x initialize interface port1.0.2
```

To unauthorize switch `port1.0.1` and attempt reauthentication on switch `port1.0.1`, use the command:

```
awplus# dot1x initialize interface port1.0.1
```

**Validation Commands** `show dot1x`  
`show dot1x interface`

**Related Commands** `dot1x initialize supplicant`

# dot1x initialize supplicant

**Overview** This command removes authorization for a connected supplicant with the specified **MAC address** or **username**. The connection will attempt to re-authorize when the specified supplicant attempts to make use of the network connection.

**NOTE:** Reauthentication could be a long time after the use of this command because the reauthorization attempt is not triggered by this command. The attempt is triggered by the first packet from the supplicant trying to access the network resources.

**Syntax** dot1x initialize supplicant {<macadd>|username}

| Parameter  | Description                                      |
|------------|--------------------------------------------------|
| dot1x      | IEEE 802.1X Port-Based Access Control.           |
| initialize | Initialize the port to attempt reauthentication. |
| supplicant | Specify the supplicant to initialize.            |
| <macadd>   | MAC (hardware address of the supplicant.         |
| username   | The name of the supplicant entry.                |

**Mode** Privileged Exec

**Example** To initialize the supplicant authentication, use the commands

```
awplus# configure terminal
awplus(config)# dot1x initialize supplicant 0090.99ab.a020
awplus(config)# dot1x initialize supplicant guest
```

**Validation Commands** [show dot1x](#)  
[show dot1x supplicant](#)

**Related Commands** [dot1x initialize interface](#)

# dot1x keytransmit

**Overview** This command enables key transmission on the interface specified previously in Interface mode.

The **no** variant of this command disables key transmission on the interface specified.

**Syntax** dot1x keytransmit  
no dot1x keytransmit

**Default** Key transmission for port authentication is enabled by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** Use this command to enable key transmission over an Extensible Authentication Protocol (EAP) packet between the authenticator and supplicant. Use the **no** variant of this command to disable key transmission.

**Examples** To enable the key transmit feature on interface port1.0.2, after it has been disabled by negation, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x keytransmit
```

To disable the key transmit feature from the default startup configuration on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x keytransmit
```

**Validation  
Commands** show dot1x  
show dot1x interface

# dot1x max-auth-fail

**Overview** Use this command to configure the maximum number of login attempts for a supplicant (client device) using the **auth-fail vlan** feature, when using 802.1X port authentication on an interface.

The **no** variant of this command resets the maximum login attempts for a supplicant (client device) using the auth-fail vlan feature, to the default configuration of 3 login attempts.

**Syntax** dot1x max-auth-fail <0-10>  
no dot1x max-auth-fail

| Parameter | Description                                                                                                    |
|-----------|----------------------------------------------------------------------------------------------------------------|
| <0-10>    | Specify the maximum number of login attempts for supplicants on an interface using 802.1X port authentication. |

**Default** The default maximum number of login attempts for a supplicant on an interface using 802.1X port authentication is three (3) login attempts.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** This command sets the maximum number of login attempts for supplicants on an interface. The supplicant is moved to the auth-fail VLAN from the Guest VLAN after the number of failed login attempts using 802.1X authentication is equal to the number set with this command.

See the [Authentication Feature Overview and Configuration Guide](#) for information about:

- the auth-fail VLAN feature, and
- restrictions regarding combinations of authentication enhancements working together

**Examples** To configure the maximum number of login attempts for a supplicant on interface port1.0.2 to a single (1) login attempt, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x max-auth-fail 1
```

To configure the maximum number of login attempts for a supplicant on interface port1.0.2 to the default number of three (3) login attempts, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x max-auth-fail
```

**Validation  
Commands**    `show running-config`

**Related  
Commands**    `auth auth-fail vlan`  
                  `dot1x max-reauth-req`  
                  `show dot1x interface`



# dot1x max-reauth-req

**Overview** This command sets the number of reauthentication attempts before an interface is unauthorized.

The **no** variant of this command resets the reauthentication delay to the default.

**Syntax** dot1x max-reauth-req <1-10>  
no dot1x max-reauth-req

| Parameter | Description                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------|
| <1-10>    | Specify the maximum number of reauthentication attempts for supplicants on an interface using 802.1X port authentication. |

**Default** The default maximum reauthentication attempts for interfaces using 802.1X port authentication is two (2) reauthentication attempts, before an interface is unauthorized.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** Use this command to set the maximum reauthentication attempts after failure.

**Examples** To configure the maximum number of reauthentication attempts for interface port1.0.2 to a single (1) reauthentication request, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x max-reauth-req 1
```

To configure the maximum number of reauthentication attempts for interface port1.0.2 to the default maximum number of two (2) reauthentication attempts, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x max-reauth-req
```

**Validation Commands** show running-config

**Related Commands** dot1x max-auth-fail  
show dot1x interface

# dot1x port-control

**Overview** This command enables 802.1X port authentication on the interface specified, and sets the control of the authentication port. 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.

The **no** variant of this command disables the port authentication on the interface specified.

**Syntax** dot1x port-control {force-unauthorized|force-authorized|auto}  
no dot1x port-control

| Parameter          | Description                                                                                         |
|--------------------|-----------------------------------------------------------------------------------------------------|
| force-unauthorized | Force port state to unauthorized.<br>Specify to force a port to always be in an unauthorized state. |
| force-authorized   | Force port state to authorized.<br>Specify to force a port to always be in an authorized state.     |
| auto               | Allow port client to negotiate authentication.<br>Specify to enable authentication on port.         |

**Default** 802.1X port control is disabled by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** Use this command to force a port state. Note that all **dot1x** commands can only be applied to switch ports. They cannot be applied to dynamic (LACP) or static channel groups.

**Examples** To enable port authentication on the interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
```

To enable port authentication force authorized on the interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control force-authorized
```

To disable port authentication on the interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x port-control
```

**Validation  
Commands**    [show dot1x interface](#)

**Related  
Commands**    [aaa authentication dot1x](#)

# dot1x timeout tx-period

**Overview** This command sets the transmit timeout for the authentication request on the specified interface.

The **no** variant of this command resets the transmit timeout period to the default (30 seconds).

**Syntax** dot1x timeout tx-period <1-65535>  
no dot1x timeout tx-period

| Parameter | Description |
|-----------|-------------|
| <1-65535> | Seconds.    |

**Default** The default transmit period for port authentication is 30 seconds.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** Use this command to set the interval between successive attempts to request an ID.

**Examples** To set the transmit timeout period to 5 seconds on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x timeout tx-period 5
```

To reset transmit timeout period to the default (30 seconds) on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x timeout tx-period
```

**Validation Commands** show dot1x  
show dot1x interface

# show debugging dot1x

**Overview** Use this command to display the 802.1X debugging option set.

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 debugging dot1x

**Mode** User Exec and Privileged Exec

**Usage** This is a sample output from the show debugging dot1x command.

```
awplus# debug dot1x
awplus# show debugging dot1x
```

```
802.1X debugging status:

802.1X events debugging is on

802.1X timer debugging is on

802.1X packets debugging is on

802.1X NSM debugging is on
```

**Example** awplus# show debugging dot1x

**Related Commands** [debug dot1x](#)

# show dot1x

**Overview** This command shows authentication information for dot1x (802.1X) port authentication.

If you specify the optional **all** parameter then this command also displays all authentication information for each port available on the switch.

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 dot1x [all]

| Parameter | Description                                                                    |
|-----------|--------------------------------------------------------------------------------|
| all       | Displays all authentication information for each port available on the switch. |

**Mode** Privileged Exec

**Example** awplus# show dot1x all

Table 27-1: Example output from the **show dot1x** command

```
awplus# show dot1x all
802.1X Port-Based Authentication Enabled
RADIUS server address: 150.87.18.89:1812
Next radius message id: 5
RADIUS client address: not configured
Authentication info for interface port1.0.6
portEnabled: true - portControl: Auto
portStatus: Authorized
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
dynamicVlanCreation: single-dynamic-vlan
assignFailActionRule: deny
hostMode: multi-supPLICANT
maxSupPLICANT: 256
dot1x: enabled
protocolVersion: 1
authMac: enabled
method: PAP
reauthRelearning: disabled
authWeb: enabled
method: PAP
lockCount: 3
packetForwarding: disabled
twoStepAuthentication:
 configured: enabled
 actual: enabled
SupPLICANTMac: none
```

Table 27-1: Example output from the **show dot1x** command (cont.)

```

supplicantMac: none
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
 authenticationMethod: 802.1X Authentication
 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 - txPeriod: 30
 BE: state: Idle - reqCount: 0 - idFromServer: 0
 CD: adminControlledDirections: in - operControlledDirections: in
 CD: bridgeDetected: false
 KR: rxKey: false
 KT: keyAvailable: false - keyTxEnabled: false
 criticalState: off
 dynamicVlanId: 2
802.1X statistics for interface port1.0.6
 EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
 EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
 EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
 EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
 Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
 EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame Src: 00d0.59ab.7037
Authentication session statistics for interface port1.0.6
 session user name: manager
 session authentication method: Remote server
 session time: 19440 secs
 session terminate cause: Not terminated yet
Authentication Diagnostics for interface port1.0.6
 Supplicant address: 00d0.59ab.7037
 authEnterConnecting: 2
 authEaplogoffWhileConnecting: 1
 authEnterAuthenticating: 2
 authSuccessWhileAuthenticating: 1
 authTimeoutWhileAuthenticating: 1
 authFailWhileAuthenticating: 0
 authEapstartWhileAuthenticating: 0
 authEaploggogWhileAuthenticating: 0
 authReauthsWhileAuthenticated: 0
 authEapstartWhileAuthenticated: 0
 authEaplogoffWhileAuthenticated: 0
 BackendResponses: 2
 BackendAccessChallenges: 1
 BackendOtherrequestToSupplicant: 3
 BackendAuthSuccess: 1
 BackendAuthFails: 0

```



# show dot1x diagnostics

**Overview** This command shows 802.1X authentication diagnostics for the specified interface (optional), which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

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 dot1x diagnostics [interface <interface-list>]

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface        | Specify a port to show.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <interface-list> | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• an interface (e.g. v lan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v lan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.2-1.0.4. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |

**Mode** Privileged Exec

**Example** See the sample output below showing 802.1X authentication diagnostics for port1.0.5:

```
awplus# show dot1x diagnostics interface port1.0.5
```

**Output** Figure 27-1: Example output from the **show dot1x diagnostics** command

```
Authentication Diagnostics for interface port1.0.5
 Supplicant address: 00d0.59ab.7037
 authEnterConnecting: 2
 authEaplogoffWhileConnecting: 1
 authEnterAuthenticating: 2
 authSuccessWhileAuthenticating: 1
 authTimeoutWhileAuthenticating: 1
 authFailWhileAuthenticating: 0
 authEapstartWhileAuthenticating: 0
 authEaplogoggWhileAuthenticating: 0
 authReauthsWhileAuthenticated: 0
 authEapstartWhileAuthenticated: 0
 authEaplogoffWhileAuthenticated: 0
 BackendResponses: 2
 BackendAccessChallenges: 1
 BackendOtherrequestToSupplicant: 3
 BackendAuthSuccess: 1
```

# show dot1x interface

**Overview** This command shows the status of 802.1X port-based authentication on the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interfaces. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interfaces. Use the optional **statistics** parameter to show authentication diagnostics for the specified interfaces. Use the optional **supplicant** parameter to show the supplicant state for the specified interfaces.

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 dot1x interface <interface-list>  
[diagnostics|sessionstatistics|statistics|supplicant [brief]]

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface-list>  | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• an interface (e.g. v lan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v lan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.3-1.0.5. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |
| diagnostics       | Diagnostics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| sessionstatistics | Session Statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistics        | Statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| supplicant        | Supplicant.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| brief             | Brief summary of supplicant state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

**Mode** Privileged Exec

**Examples** See the sample output below showing 802.1X authentication status for port1.0.6:

```
awplus# show dot1x interface port1.0.6
```

Table 27-2: Example output from the **show dot1x interface** command for a port

```
awplus#show dot1x interface port1.0.6
Authentication info for interface port1.0.6
 portEnabled: true - portControl: Auto
 portStatus: Authorized
 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
 dynamicVlanCreation: single-dynamic-vlan
 assignFailActionRule: deny
 hostMode: multi-supPLICANT
 maxSupPLICANT: 256
dot1x: enabled
protocolVersion: 1
authMac: enabled
method: PAP
reauthRelearning: disabled
authWeb: enabled
method: PAP
lockCount: 3
packetForwarding: disabled
 twoStepAuthentication:
 configured: enabled
 actual: enabled
supPLICANTMac: none
```

See the sample output below showing 802.1X authentication session statistics for port1.0.6:

```
awplus# show dot1x interface port1.0.6 sessionstatistics
```

```
awplus#show dot1x interface port1.0.6
sessionstatistics
Authentication session statistics for interface
port1.0.6
 session user name: manager
 session authentication method: Remote server
 session time: 19440 secs
 session terminat cause: Not terminated yet
```

See sample output below showing 802.1X authentication diagnostics for port1.0.6:

```
awplus# show dot1x interface port1.0.6 diagnostics
```

```
awplus#show dot1x interface port1.0.6 diagnostics
Authentication Diagnostics for interface port1.0.6
 Supplicant address: 00d0.59ab.7037
 authEnterConnecting: 2
 authEaplogoffWhileConnecting: 1
 authEnterAuthenticating: 2
 authSuccessWhileAuthenticating: 1
 authTimeoutWhileAuthenticating: 1
 authFailWhileAuthenticating: 0
 authEapstartWhileAuthenticating: 0
 authEaplogoggWhileAuthenticating: 0
 authReauthsWhileAuthenticated: 0
 authEapstartWhileAuthenticated: 0
 authEaplogoffWhileAuthenticated: 0
 BackendResponses: 2
 BackendAccessChallenges: 1
 BackendOtherrequestToSupplicant: 3
 BackendAuthSuccess: 1
```

See sample output below showing the supplicant on the interface port1.0.6:

```
awplus# show dot1x interface port1.0.6 supplicant
```

```
awplus#show dot1x interface port1.0.6 supplicant
authenticationMethod: dot1x
 totalSupplicantNum: 1
 authorizedSupplicantNum: 1
 macBasedAuthenticationSupplicantNum: 0
 dot1xAuthenticationSupplicantNum: 1
 webBasedAuthenticationSupplicantNum: 0
 Supplicant name: manager
 Supplicant address: 00d0.59ab.7037
 authenticationMethod: dot1x
 portStatus: Authorized - currentId: 4
 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 - txPeriod: 30
 BE: state: Idle - reqCount: 0 - idFromServer: 3
 BE: supTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in -
 operControlledDirections: in
 CD: bridgeDetected: false
 KR: rxKey: false
 KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing 802.1X (dot1x) authentication statistics for port1.0.6:

awplus# show dot1x statistics interface port1.0.6

```
awplus#show dot1x statistics interface port1.0.6
802.1X statistics
for interface port1.0.6
 EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
 EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
 EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
 EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
 Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
 EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame
Src:00d0.59ab.7037
```

Table 27-3: Parameters in the output of **show dot1x interface**

| Parameter      | Description                                                       |
|----------------|-------------------------------------------------------------------|
| portEnabled    | Interface operational status (Up-true/down-false).                |
| portControl    | Current control status of the port for 802.1X control.            |
| portStatus     | 802.1X status of the port (authorized/unauthorized).              |
| reAuthenticate | Reauthentication enabled/disabled status on port.                 |
| reAuthPeriod   | Value holds meaning only if reauthentication is enabled.          |
| abort          | Indicates that authentication should be aborted when set to true. |
| fail           | Indicates failed authentication attempt when set to false.        |
| start          | Indicates authentication should be started when set to true.      |
| timeout        | Indicates authentication attempt timed out when set to true.      |
| success        | Indicates authentication successful when set to true.             |
| state          | Current 802.1X operational state of interface.                    |
| mode           | Configured 802.1X mode.                                           |
| reAuthCount    | Reauthentication count.                                           |
| quietperiod    | Time between reauthentication attempts.                           |
| reAuthMax      | Maximum reauthentication attempts.                                |
| BE             | Backend authentication state machine variables and constants.     |
| state          | State of the state machine.                                       |

Table 27-3: Parameters in the output of **show dot1x interface** (cont.)

| Parameter                      | Description                                                                                            |
|--------------------------------|--------------------------------------------------------------------------------------------------------|
| reqCount                       | Count of requests sent to server.                                                                      |
| suppTimeout                    | Supplicant timeout.                                                                                    |
| serverTimeout                  | Server timeout.                                                                                        |
| maxReq                         | Maximum requests to be sent.                                                                           |
| CD                             | Controlled Directions State machine.                                                                   |
| adminControlledDir<br>rections | Administrative value (Both/In).                                                                        |
| operControlledDir<br>rections  | Operational Value (Both/In).                                                                           |
| KR                             | Key receive state machine.                                                                             |
| rxKey                          | True when EAPOL-Key message is received by supplicant or authenticator. false when key is transmitted. |
| KT                             | Ket Transmit State machine.                                                                            |
| keyAvailable                   | False when key has been transmitted by authenticator, true when new key is available for key exchange. |
| keyTxEnabled                   | Key transmission enabled/disabled status.                                                              |

**Related  
Commands**

- [show auth-web diagnostics](#)
- [show dot1x sessionstatistics](#)
- [show dot1x statistics interface](#)
- [show dot1x supplicant interface](#)

# show dot1x sessionstatistics

**Overview** This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

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 dot1x sessionstatistics [interface <interface-list>]

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface        | Specify a port to show.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <interface-list> | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• an interface (e.g. v lan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v lan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |

**Mode** Privileged Exec

**Example** See sample output below showing 802.1X (dot1x) authentication session statistics for port1.0.6:

```
awplus# show dot1x sessionstatistics interface port1.0.6
```

```
Authentication session statistics for interface
port1.0.6
 session user name: manager
 session authentication method: Remote server
 session time: 19440 secs
 session terminat cause: Not terminated yet
```



# show dot1x statistics interface

**Overview** This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

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 dot1x statistics interface *<interface-list>*

| Parameter                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;interface-list&gt;</i> | <p>The interfaces or ports to configure. An interface-list can be:</p> <ul style="list-style-type: none"><li>• an interface (e.g. v lan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v lan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</li></ul> <p>The specified interfaces must exist.</p> |

**Mode** Privileged Exec

**Example** See sample output below showing 802.1X authentication statistics for port1.0.6:

```
awplus# show dot1x statistics interface port1.0.6
```

```
802.1X statistics for interface port1.0.6
EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame
Src:00d0.59ab.7037
```

# show dot1x supplicant

**Overview** This command shows the supplicant state of the authentication mode set for the switch.

This command shows a summary when the optional **brief** parameter is used.

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 dot1x supplicant [<macadd>] [brief]

| Parameter | Description                               |
|-----------|-------------------------------------------|
| <macadd>  | MAC (hardware) address of the Supplicant. |
| brief     | Brief summary of the Supplicant state.    |

**Mode** Privileged Exec

**Example** See sample output below showing the 802.1X authenticated supplicant on the switch:

```
awplus# show dot1x supplicant
```

```
authenticationMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
 authenticationMethod: dot1x
 Two-Step Authentication:
 firstAuthentication: Pass - Method: mac
 secondAuthentication: Pass - Method: dot1x
portStatus: Authorized - currentId: 4
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 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 3
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing the supplicant on the switch using the brief parameter:

```
awplus# show dot1x supplicant 00d0.59ab.7037 brief
```

```
Interface port1.0.6
 authenticationMethod: dot1x
 totalSupplicantNum: 1
 authorizedSupplicantNum: 1
 macBasedAuthenticationSupplicantNum: 0
 dot1xAuthenticationSupplicantNum: 1
 webBasedAuthenticationSupplicantNum: 0
```

| Interface | VID | Mode | MAC Address    | Status        | IP Address    | Username |
|-----------|-----|------|----------------|---------------|---------------|----------|
| =====     | === | ===  | =====          | =====         | =====         | =====    |
| port1.0.6 |     |      |                |               |               |          |
| 2         | D   |      | 00d0.59ab.7037 | Authenticated | 192.168.2.201 | manager  |

See sample output below showing the supplicant on the switch using the brief parameter:

```
awplus# show dot1x supplicant brief
```

For example, if two-step authentication is configured with 802.1X authentication as the first method and web authentication as the second method then the output is as follows:

```
Interface port1.0.6 authenticationMethod: dot1x/web
 Two-Step Authentication
 firstMethod: dot1x
 secondMethod: web
 totalSupplicantNum: 1
 authorizedSupplicantNum: 1
 macBasedAuthenticationSupplicantNum: 0
 dot1xAuthenticationSupplicantNum: 0
 webBasedAuthenticationSupplicantNum: 1
 otherAuthenticationSupplicantNum: 0
```

| Interface | VID | Mode | MAC Address    | Status        | IP Address    | Username |
|-----------|-----|------|----------------|---------------|---------------|----------|
| =====     | === | ===  | =====          | =====         | =====         | =====    |
| port1.0.6 |     |      |                |               |               |          |
| 5         | W   |      | 0008.0d5e.c216 | Authenticated | 192.168.1.200 | web      |

**Related Commands** [show dot1x supplicant interface](#)

# show dot1x supplicant interface

**Overview** This command shows the supplicant state of the authentication mode set for the interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

This command shows a summary when the optional **brief** parameter is used.

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 dot1x supplicant interface *<interface-list>* [brief]

| Parameter                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;interface-list&gt;</i> | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• an interface (e.g. v lan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v lan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |
| brief                         | Brief summary of the Supplicant state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Mode** Privileged Exec

**Examples** See sample output below showing the supplicant on the interface port1.0.6:

awplus# show dot1x interface port1.0.6

```
Interface port1.0.6 authenticationMethod: dot1x
 totalSupplicantNum: 1
 authorizedSupplicantNum: 1
 macBasedAuthenticationSupplicantNum: 0
 dot1xAuthenticationSupplicantNum: 1
 webBasedAuthenticationSupplicantNum: 0
 otherAuthenticationSupplicantNum: 0

Supplicant name: VCSPCVLAN10
Supplicant address: 0000.cd07.7b60
 authenticationMethod: 802.1X
Two-Step Authentication:
 firstAuthentication: Pass - Method: mac
 secondAuthentication: Pass - Method: dot1x
portStatus: Authorized - currentId: 3
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: 2
CD: adminControlledDirections:in -
operControlledDirections:in
 CD: bridgeDetected: false
 KR: rxKey: false
 KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing the supplicant on the switch using the brief parameter:

awplus# show dot1x supplicant interface brief

```
Interface port1.0.6
 authenticationMethod: dot1x
Two-Step Authentication:
 firstMethod: mac
 secondMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0
```

| Interface | VID | Mode | MAC Address    | Status        | IP Address    | Username |
|-----------|-----|------|----------------|---------------|---------------|----------|
| port1.0.6 |     |      |                |               |               |          |
| 2 D       |     |      | 00d0.59ab.7037 | Authenticated | 192.168.2.201 | manager  |

See the sample output below for static channel group (static aggregator) interface sa1:

awplus# show dot1x interface sa1 supplicant brief

```
awplus#show dot1x interface sa1 supplicant brief
Interface sa1
 authenticationMethod: dot1x
Two-Step Authentication:
 firstMethod: mac
 secondMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
 macBasedAuthenticationSupplicantNum: 0
 dot1xAuthenticationSupplicantNum: 1
 webBasedAuthenticationSupplicantNum: 0
 otherAuthenticationSupplicantNum: 0
```

| Interface | VID   | Mode  | MAC Address    | Status        | IP Address | Username |
|-----------|-------|-------|----------------|---------------|------------|----------|
| =====     | ===== | ===== | =====          | =====         | =====      | =====    |
| sa1       | 1     | D     | 00d0.59ab.7037 | Authenticated | --         | test1    |

**Related** [show dot1x supplicant](#)  
**Commands**

# undebug dot1x

**Overview** This command applies the functionality of the **no** variant of the [debug dot1x](#) command.

# 28

# Authentication Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for authentication commands.

- Command List**
- “auth auth-fail vlan” on page 851
  - “auth critical” on page 853
  - “auth dynamic-vlan-creation” on page 854
  - “auth guest-vlan” on page 857
  - “auth host-mode” on page 859
  - “auth log” on page 861
  - “auth max-suppliant” on page 863
  - “auth reauthentication” on page 864
  - “auth roaming disconnected” on page 865
  - “auth roaming enable” on page 867
  - “auth suppliant-mac” on page 869
  - “auth timeout connect-timeout” on page 871
  - “auth timeout quiet-period” on page 872
  - “auth timeout reauth-period” on page 873
  - “auth timeout server-timeout” on page 874
  - “auth timeout supp-timeout” on page 875
  - “auth two-step enable” on page 876
  - “auth-mac enable” on page 879
  - “auth-mac method” on page 881
  - “auth-mac password” on page 882
  - “auth-mac reauth-relearning” on page 883



- [“auth-web enable”](#) on page 884
- [“auth-web forward”](#) on page 885
- [“auth-web max-auth-fail”](#) on page 887
- [“auth-web method”](#) on page 888
- [“auth-web-server blocking-mode”](#) on page 889
- [“auth-web-server dhcp ipaddress”](#) on page 890
- [“auth-web-server dhcp lease”](#) on page 891
- [“auth-web-server dhcp-wpad-option”](#) on page 892
- [“auth-web-server gateway \(deleted\)”](#) on page 893
- [“auth-web-server host-name”](#) on page 894
- [“auth-web-server http-redirect \(deleted\)”](#) on page 895
- [“auth-web-server intercept-port”](#) on page 896
- [“auth-web-server ipaddress”](#) on page 897
- [“auth-web-server login-url”](#) on page 898
- [“auth-web-server mode \(deleted\)”](#) on page 899
- [“auth-web-server page logo”](#) on page 900
- [“auth-web-server page sub-title”](#) on page 901
- [“auth-web-server page success-message”](#) on page 902
- [“auth-web-server page title”](#) on page 903
- [“auth-web-server page welcome-message”](#) on page 904
- [“auth-web-server ping-poll enable”](#) on page 905
- [“auth-web-server ping-poll failcount”](#) on page 906
- [“auth-web-server ping-poll interval”](#) on page 907
- [“auth-web-server ping-poll reauth-timer-refresh”](#) on page 908
- [“auth-web-server ping-poll timeout”](#) on page 909
- [“auth-web-server port”](#) on page 910
- [“auth-web-server redirect-delay-time”](#) on page 911
- [“auth-web-server redirect-url”](#) on page 912
- [“auth-web-server session-keep”](#) on page 913
- [“auth-web-server ssl”](#) on page 914
- [“auth-web-server sslport \(deleted\)”](#) on page 915
- [“auth-web-server ssl intercept-port”](#) on page 916
- [“copy proxy-autoconfig-file”](#) on page 917
- [“copy web-auth-https-file”](#) on page 918
- [“erase proxy-autoconfig-file”](#) on page 919

- [“erase web-auth-https-file”](#) on page 920
- [“show auth two-step supplicant brief”](#) on page 921
- [“show auth-mac”](#) on page 922
- [“show auth-mac diagnostics”](#) on page 923
- [“show auth-mac interface”](#) on page 924
- [“show auth-mac sessionstatistics”](#) on page 926
- [“show auth-mac statistics interface”](#) on page 927
- [“show auth-mac supplicant”](#) on page 928
- [“show auth-mac supplicant interface”](#) on page 929
- [“show auth-web”](#) on page 930
- [“show auth-web diagnostics”](#) on page 932
- [“show auth-web interface”](#) on page 934
- [“show auth-web sessionstatistics”](#) on page 937
- [“show auth-web statistics interface”](#) on page 938
- [“show auth-web supplicant”](#) on page 939
- [“show auth-web supplicant interface”](#) on page 940
- [“show auth-web-server”](#) on page 941
- [“show auth-web-server page”](#) on page 942
- [“show proxy-autoconfig-file”](#) on page 943

# auth auth-fail vlan

**Overview** Use this command to enable the **auth-fail vlan** feature on the specified vlan interface. This feature assigns supplicants (client devices) to the specified VLAN if they fail port authentication.

Use the **no** variant of this command to disable the **auth-fail vlan** feature for a specified VLAN interface.

**Syntax** `auth auth-fail vlan <1-4094>`  
`no auth auth-fail vlan`

| Parameter  | Description                                                                  |
|------------|------------------------------------------------------------------------------|
| <1 - 4094> | Assigns the VLAN ID to any supplicants that have failed port authentication. |

**Default** The **auth-fail vlan** feature is disabled by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** Use the **auth-fail vlan** feature when using Web-Authentication instead of the Guest VLAN feature, when you need to separate networks where one supplicant (client device) requires authentication and another supplicant does not require authentication from the same interface.

This is because the DHCP lease time using the Web-Authentication feature is shorter, and the **auth fail vlan** feature enables assignment to a different VLAN if a supplicant fails authentication.

To enable the **auth-fail vlan** feature with Web Authentication, you need to set Web Authentication Server virtual IP address by using the [auth-web-server ipaddress](#) command or the [auth-web-server dhcp ipaddress](#) command.

When using 802.1X port authentication, use a [dot1x max-auth-fail](#) command to set the maximum number of login attempts. Three login attempts are allowed by default for 802.1X port authentication before supplicants trying to authenticate are moved from the Guest VLAN to the auth-fail VLAN. See the [dot1x max-auth-fail](#) on page 823 for command information.

See the [Authentication Feature Overview and Configuration Guide](#) for information about:

- the auth-fail VLAN feature, which allows the Network Administrator to separate the supplicants who attempted authentication, but failed, from the supplicants who did not attempt authentication, and
- restrictions regarding combinations of authentication enhancements working together

Use appropriate ACLs (Access Control Lists) on interfaces for extra security if a supplicant allocated to the designated auth-fail vlan can access the same network

as a supplicant on the Guest VLAN. For more information about ACL concepts, and configuring ACLs see the [ACL Feature Overview and Configuration Guide](#). For more information about ACL commands see:

**Examples** To enable **auth-fail vlan** for port1.0.2 and assign VLAN 100, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth auth-fail vlan 100
```

To disable the **auth-fail vlan** feature for port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth auth-fail vlan
```

**Validation  
Commands** [show running-config](#)

**Related  
Commands** [dot1x max-auth-fail](#)  
[show dot1x](#)  
[show dot1x interface](#)

# auth critical

**Overview** This command enables the critical port feature on the interface. When the critical port feature is enabled on an interface, and all the RADIUS servers are unavailable, then the interface becomes authorized.

The **no** variant of this command disables critical port feature on the interface.

**Syntax** `auth critical`  
`no auth critical`

**Default** The critical port of port authentication is disabled.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To enable the critical port feature on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth critical
```

To disable the critical port feature on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth critical
```

**Validation  
Commands** `show auth-web-server`  
`show dot1x`  
`show dot1x interface`  
`show running-config`

# auth dynamic-vlan-creation

**Overview** This command enables and disables the Dynamic VLAN assignment feature.

The Dynamic VLAN assignment feature allows a supplicant (client device) to be placed into a specific VLAN based on information returned from the RADIUS server during authentication, on a given interface.

Use the **no** variant of this command to disable the Dynamic VLAN assignment feature.

**Syntax** `auth dynamic-vlan-creation [rule {deny|permit}] [type {multi|single}]`  
`no auth dynamic-vlan-creation`

| Parameter | Description                                                                                                                                                                                |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| rule      | VLAN assignment rule.                                                                                                                                                                      |
| deny      | Deny a differently assigned VLAN ID. This is the default rule.                                                                                                                             |
| permit    | Permit a differently assigned VLAN ID.                                                                                                                                                     |
| type      | Specifies whether multiple different VLANs can be assigned to supplicants (client devices) attached to the port, or whether only a single VLAN can be assigned to supplicants on the port. |
| multi     | Multiple Dynamic VLAN.                                                                                                                                                                     |
| single    | Single Dynamic VLAN.                                                                                                                                                                       |

**Default** By default, the Dynamic VLAN assignment feature is disabled.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** If the Dynamic VLAN assignment feature is enabled (disabled by default), VLAN assignment is dynamic. If the Dynamic VLAN assignment feature is disabled then RADIUS attributes are ignored and configured VLANs are assigned to ports. Dynamic VLANs may be associated with authenticated MAC addresses if the **type** parameter is applied with the **rule** parameter.

The **rule** parameter deals with the case where there are multiple supplicants attached to a port, and the type parameter has been set to **single-vlan**. The parameter specifies how the switch should act if different VLAN IDs end up being assigned to different supplicants. The keyword value **deny** means that once a given VID has been assigned to the first supplicant, then if any subsequent supplicant is assigned a different VID, that supplicant is rejected. The keyword value **permit** means that once a given VID has been assigned to the first supplicant, then if any subsequent supplicant is assigned a different VID, that supplicant is accepted, but it is actually assigned the same VID as the first supplicant.

If you issue an **auth dynamic-vlan-creation** command without an optional **rule** parameter and a required **deny** or **permit** keyword value then a second supplicant with a different VLAN ID is rejected. It is not assigned to the first supplicant's VLAN. Issuing an **auth dynamic-vlan-creation** command without an optional **rule** parameter has the same effect as issuing an **auth dynamic-vlan-creation rule deny** command rejecting supplicants with differing VLANs.

The **type** parameter specifies whether multiple different VLANs can be assigned to supplicants attached to the port, or whether only a single VLAN can be assigned to supplicants on the port. The **type** parameter can select the port base VLAN or the MAC base VLAN from the RADIUS VLAN ID. This can be used when the host-mode is set to multi-supplicant. For **single**-host ports, the VLAN ID will be assigned to the port. It is not supported with the Guest VLAN feature. Display the ID assigned using a **show vlan** command. For **multi**-host ports, the VLAN ID will be assigned to the MAC address of the authenticated supplicant. The VLAN ID assigned for the MAC Base VLAN is displayed using the **show platform table vlan** command.

To configure Dynamic Vlan with Web Authentication, you need to set Web Authentication Server virtual IP address by using the [auth-web-server ipaddress](#) command or the [auth-web-server dhcp ipaddress](#) command. You also need to create a hardware access-list that can be applied to the switch port interface.

You need to configure an IPv4 address for the VLAN interface on which Web Authentication is running.

**Examples** To enable the Dynamic VLAN assignment feature on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport access vlan 10
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# interface vlan10
awplus(config-if)# ip address 10.1.1.1/24
```

To enable the Dynamic VLAN assignment feature with Web Authentication on interface port1.0.2 when Web Authentication is needed, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ipaddress 1.2.3.4
awplus(config)# access-list hardware acl-web send-to-cpu ip any 1.2.3.4
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# access-group acl-web
awplus(config-if)# interface vlan1
awplus(config-if)# ip address 10.1.1.1/24
```

To disable the Dynamic VLAN assignment feature on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth dynamic-vlan-creation
```

**Validation  
Commands**

```
show dot1x
show dot1x interface
show running-config
```

**Related  
Commands**

```
auth host-mode
```



## auth guest-vlan

**Overview** This command enables and configures the Guest VLAN feature on the interface specified by associating a Guest VLAN with an interface. This command does not start authentication. The supplicant's (client device's) traffic is associated with the native VLAN of the interface if its not already associated with another VLAN. The **routing** option enables routing from the Guest VLAN to another VLAN, so the switch can lease DHCP addresses and accept access to a limited network.

The **no** variant of this command disables the guest vlan feature on the interface specified.

**Syntax** `auth guest-vlan <1-4094> [routing]`  
`no auth guest-vlan [routing]`

| Parameter  | Description                                         |
|------------|-----------------------------------------------------|
| <1 - 4094> | VLAN ID (VID).                                      |
| routing    | Enables routing from the Guest VLAN to other VLANs. |

**Default** The Guest VLAN authentication feature is disabled by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** The Guest VLAN feature may be used by supplicants (client devices) that have not attempted authentication, or have failed the authentication process. Note that if a port is in multi-supplicant mode with per-port dynamic VLAN configuration, after the first successful authentication, subsequent hosts cannot use the guest VLAN due to the change in VLAN ID. This may be avoided by using per-user dynamic VLAN assignment.

When using the Guest VLAN feature with the multi-host mode, a number of supplicants can communicate via a guest VLAN before authentication. A supplicant's traffic is associated with the native VLAN of the specified switch port. The supplicant must belong to a VLAN before traffic from the supplicant can be associated.

Note that you must first define the VLAN with the **vlan** command that you will assign as a guest VLAN using this command. Also note that 802.1X must first be enabled on the port.

Guest VLAN authentication cannot be enabled if DHCP snooping is enabled ([service dhcp-snooping](#) command), and vice versa.

The Guest VLAN feature in previous releases had some limitations that have been removed. Until this release the Guest VLAN feature could not lease the IP address to the supplicant using DHCP Server or DHCP Relay features unless Web-Authentication was also applied. When using NAP authentication, the supplicant should have been able to log on to a domain controller to gain certification, but the Guest VLAN would not accept access to another VLAN.

The Guest VLAN routing mode in this release overcomes these issues. With the Guest VLAN routing mode, the switch can lease DHCP addresses and accept access to a limited network.

Note that Guest VLAN can use only untagged ports and tagged ports cannot be used for Guest VLAN.

See the [Authentication Feature Overview and Configuration Guide](#) for information about:

- Guest VLAN, and
- restrictions regarding combinations of authentication enhancements working together

**Examples** To define `vlan100` and assign the guest VLAN feature to `vlan100` on interface `port1.0.2`, and enable routing from the guest vlan to other VLANs, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 100
awplus(config-vlan)# exit
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth guest-vlan 100 routing
```

To disable the guest vlan feature on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth guest-vlan
```

**Validation  
Commands** [show dot1x](#)  
[show dot1x interface](#)  
[show running-config](#)

**Related  
Commands** [dot1x port-control](#)  
[vlan](#)

## auth host-mode

**Overview** This command selects host mode on the interface. Multi-host is an extension to IEEE802.1X.

Use the **no** variant of this command to set host mode to the default setting (single host).

**Syntax** `auth host-mode {single-host|multi-host|multi-supPLICant}`  
`no auth host-mode`

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| single-host      | Single host mode. In this mode, only one host may be authorized with the port. If other hosts out the interface attempt to authenticate, the authenticator blocks the attempt.                                                                                                                                                                                                                                                                                            |
| multi-host       | Multi host mode. In this mode, multiple hosts may be authorized with the port; however only one host must be successfully authenticated at the Authentication Server for all hosts to be authorized with the port. Upon one host being successfully authenticated (state Authenticated), the other hosts will be automatically authorized at the port (state ForceAuthorized). If no host is successfully authenticated, then all hosts are not authorized with the port. |
| multi-supPLICant | Multi supplicant (client device) mode. In this mode, multiple hosts may be authorized with the port, but each host must be individually authenticated with the Authentication Server to be authorized with the port. Supplicants which are not authenticated are not authorized with the port, while supplicants which are successfully authenticated are authorized with the port.                                                                                       |

**Default** The default host mode for port authentication is for a single host.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** Ports residing in the unauthorized state for host(s) or supplicant(s), change to an authorized state when the host or supplicant has successfully authenticated with the Authentication Server.

When multi-host mode is used or auth critical feature is used, all hosts do not need to be authenticated.

**Examples** To set the host mode to multi-supPLICANT on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth host-mode multi-supPLICANT
```

To set the host mode to default (single host) on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth host-mode
```

**Validation  
Commands** `show dot1x`  
`show dot1x interface`  
`show running-config`

# auth log

**Overview** Use this command to configure the types of authentication feature log messages that are output to the log file.

Use the **no** variant of this command to remove either specified types or all types of authentication feature log messages that are output to the log file.

**Syntax** `auth log {dot1x|auth-mac|auth-web}  
{success|failure|logoff|all}`  
`no auth log {dot1x|auth-mac|auth-web}  
{success|failure|logoff|all}`

| Parameter | Description                                                                                                                                                 |
|-----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| dot1x     | Specify only 802.1X-Authentication log messages are output to the log file.                                                                                 |
| auth-mac  | Specify only MAC-Authentication log messages are output to the log file.                                                                                    |
| auth-web  | Specify only Web-Authentication log messages are output to the log file.                                                                                    |
| success   | Specify only successful authentication log messages are output to the log file.                                                                             |
| failure   | Specify only authentication failure log messages are output to the log file.                                                                                |
| logoff    | Specify only authentication log-off messages are output to the log file. Note that link down, age out and expired ping polling messages will be included.   |
| all       | Specify all types of authentication log messages are output to the log file. Note that this is the default behavior for the authentication logging feature. |

**Default** All types of authentication log messages are output to the log file by default.

**Mode** Interface Configuration

**Examples** To configure the logging of MAC-Authentication failures to the log file for supplicants (client devices) connected to interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth log auth-mac failure
```

To configure the logging of all types of authentication log messages to the log file for supplicants (client devices) connected to interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth log all
```

**Validation**    `show running-config`  
**Commands**

# auth max-suppliant

**Overview** This command sets the maximum number of supplicants (client devices) on the interface that can be authenticated. After this value is exceeded supplicants are not authenticated.

The **no** variant of this command resets the maximum supplicant number to the default (1024).

**Syntax** `auth max-suppliant <2-1024>`  
`no auth max-suppliant`

| Parameter                   | Description   |
|-----------------------------|---------------|
| <code>&lt;2-1024&gt;</code> | Limit number. |

**Default** The max supplicant of port authentication is 1024.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To set the maximum number of supplicants to 10 on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth max-suppliant 10
```

To reset the maximum number of supplicant to default on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth max-suppliant
```

**Validation  
Commands** `show dot1x`  
`show dot1x interface`  
`show running-config`

# auth reauthentication

**Overview** This command enables re-authentication on the interface specified in the Interface mode, which may be a static channel group (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the **no** variant of this command to disables reauthentication on the interface.

**Syntax** auth reauthentication  
no auth reauthentication

**Default** Reauthentication of port authentication is disabled by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To enable reauthentication on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth reauthentication
```

**Validation  
Commands** show dot1x  
show dot1x interface  
show running-config



# auth roaming disconnected

**Overview** This command enables the Roaming Authentication feature on an authenticated interface that is link down. A supplicant (a client device) is not reauthenticated when moved between authenticated interfaces, providing both interfaces have the Roaming Authentication feature enabled before the supplicant is moved.

Use the [auth roaming enable](#) command before using this command. The [auth roaming disconnected](#) command on its own will have no effect on the operation of the switch. This command will only come into effect once the base Roaming Authentication feature is enabled, using the [auth roaming enable](#) command.

The **no** variant of this command disables the Roaming Authentication feature on an interface, and forces a supplicant to be reauthenticated when moving between interfaces.

See the [Authentication Feature Overview and Configuration Guide](#) for further information about this feature.

**Syntax** `auth roaming disconnected`  
`no auth roaming disconnected`

**Default** The Roaming Authentication `disconnected` feature is disabled by default on an interface. Authentication status for a roaming supplicant is deleted by default when an interface goes down.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** This command allows a supplicant to move to another authenticating interface without reauthentication, if the link is down for the interface that the supplicant is moved from.

Note that 802.1X port authentication, or MAC-Authentication, or Web-Authentication must first be enabled on an interface to use this feature. The port that the supplicant is moving to must have the same authentication configuration as the port the supplicant is moving from.

Configure [auth roaming enable](#) on an interface before configuring [auth roaming disconnected](#) if you require [auth roaming disconnected](#) configured on an interface for a roaming supplicant.

Roaming Authentication cannot be enabled if DHCP snooping is enabled ([service dhcp-snooping](#) command), and vice versa.

**Examples** To enable Roaming Authentication disconnected feature for port1.0.2, after enabling 802.1X-Authentication and enabling Roaming Authentication enable, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth roaming enable
awplus(config-if)# auth roaming disconnected
```

To disable Roaming Authentication disconnected feature for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth roaming disconnected
```

**Validation  
Commands** `show running-config`

**Related  
Commands** `auth-mac enable`  
`auth roaming enable`  
`auth-web enable`  
`dot1x port-control`  
`show auth-mac interface`  
`show auth-web interface`  
`show dot1x interface`

# auth roaming enable

**Overview** This command enables the Roaming Authentication feature on an authenticated interface that is link up. A supplicant (a client device) is not reauthenticated when moved between authenticated interfaces, providing both interfaces have the Roaming Authentication feature enabled before the supplicant is moved.

Use the [auth roaming enable](#) command before using [auth roaming disconnected](#) command. The [auth roaming disconnected](#) command on its own will have no effect on the operation of the switch. This command will only come into effect once the base Roaming Authentication feature is enabled, using the [auth roaming enable](#) command.

The **no** variant of this command disables the Roaming Authentication feature on an interface, and forces a supplicant to be reauthenticated when moving between interfaces.

See the [Authentication Feature Overview and Configuration Guide](#) for further information about this feature.

**Syntax** `auth roaming enable`  
`no auth roaming enable`

**Default** The Roaming Authentication enable feature is disabled by default on an interface. Authentication status for a roaming supplicant is deleted by default when an interface goes down.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** This command allows a supplicant to move to another authenticating interface without reauthentication, providing the link is up for the interface that the supplicant is moved from.

Note that 802.1X port authentication, or MAC-Authentication, or Web-Authentication must first be enabled on an interface to use this feature. The port that the supplicant is moving to must have the same authentication configuration as the port the supplicant is moving from.

Configure [auth roaming enable](#) on an interface before configuring [auth roaming disconnected](#) if you require [auth roaming disconnected](#) configured on an interface for a roaming supplicant.

Roaming Authentication cannot be enabled if DHCP snooping is enabled ([service dhcp-snooping](#) command), and vice versa.

**Examples** To enable the Roaming Authentication enable feature for interface port1.0.4, after enabling 802.1X-Authentication, since an authentication method is required, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth roaming enable
```

To disable Roaming Authentication enable for port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no auth roaming enable
```

**Validation  
Commands** [show running-config](#)

**Related  
Commands** [auth-mac enable](#)  
[auth roaming disconnected](#)  
[auth-web enable](#)  
[dot1x port-control](#)  
[show auth-mac interface](#)  
[show auth-web interface](#)  
[show dot1x interface](#)

# auth supplicant-mac

**Overview** This command adds a supplicant (client device) MAC address on a given interface with the parameters as specified in the table below.

Use the **no** variant of this command to delete the supplicant MAC address added by the **auth supplicant-mac** command, and resets to the default for the supplicant parameter.

**Syntax** `auth supplicant <mac-addr> [max-reauth-req <1-10>]  
[port-control  
{auto|force-authorized|force-unauthorized|skip-second-auth}]  
[quiet-period <1-65535>] [reauth-period <1-4294967295>]  
[supp-timeout <1-65535>] [server-timeout <1-65535>]  
[reauthentication]  
no auth supplicant-mac <macadd> [reauthentication]`

| Parameter          | Description                                                                                      |
|--------------------|--------------------------------------------------------------------------------------------------|
| <mac-addr>         | MAC (hardware) address of the Supplicant entry in HHHH.HHHH.HHHH MAC address hexadecimal format. |
| port-control       | Port control commands.                                                                           |
| auto               | Allow port client to negotiate authentication.                                                   |
| force-authorized   | Force port state to authorized.                                                                  |
| force-unauthorized | Force port state to unauthorized.                                                                |
| skip-second-auth   | Skip the second authentication.                                                                  |
| quiet-period       | Quiet period in the HELD state (default 60 seconds).                                             |
| <1-65535>          | Seconds for quiet period.                                                                        |
| reauth-period      | Seconds between reauthorization attempts (default 3600 seconds).                                 |
| <1-4294967295>     | Seconds for reauthorization attempts (reauth-period).                                            |
| supp-timeout       | Supplicant response timeout (default 30 seconds).                                                |
| <1-65535>          | Seconds for supplicant response timeout.                                                         |
| server-timeout     | Authentication server response timeout (default 30 seconds).                                     |
| <1-65535>          | Seconds for authentication server response timeout.                                              |
| reauthentication   | Enable reauthentication on a port.                                                               |
| max-reauth-req     | No of reauthentication attempts before becoming unauthorized (default 2).                        |
| <1-10>             | Count of reauthentication attempts.                                                              |

**Default** No supplicant MAC address for port authentication exists by default until first created with the **auth supplicant-mac** command. The defaults for parameters applied are as shown in the table.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To add the supplicant MAC address 0009 . 41A4 . 5943 to force authorized port control for interface port1 . 0 . 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth supplicant-mac 0009.41A4.5943
port-control force-authorized
```

To delete the supplicant MAC address 0009 . 41A4 . 5943 for interface port1 . 0 . 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-mac 0009.41A4.5943
```

To reset reauthentication to disable for the supplicant MAC address 0009 . 41A4 . 5943, for interface port1 . 0 . 2 use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-mac 0009.41A4.5943
reauthentication
```

**Validation** [show dot1x](#)  
**Commands** [show dot1x interface](#)  
[show running-config](#)

# auth timeout connect-timeout

**Overview** This command sets the connect-timeout period for the interface.

Use the **no** variant of this command to reset the connect-timeout period to the default (30 seconds).

**Syntax** `auth timeout connect-timeout <1-65535>`  
`no auth timeout connect-timeout`

| Parameter | Description |
|-----------|-------------|
| <1-65535> | Seconds.    |

**Default** The connect-timeout default is 30 seconds.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** This command is used for MAC- and Web-Authentication. If the connect-timeout has lapsed and the supplicant has the state **connecting**, then the supplicant is deleted. When [auth-web-server session-keep](#) or [auth two-step enable](#) is enabled, we recommend you configure a longer connect-timeout period.

**Examples** To set the connect-timeout period to 3600 for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout connect-timeout 3600
```

To reset the connect-timeout period to the default (30 seconds) for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout connect-timeout
```

**Validation Commands** `show dot1x`  
`show dot1x interface`

# auth timeout quiet-period

**Overview** This command sets the time period for which the authentication request is not accepted on a given interface, after the authentication request has failed an authentication.

Use the **no** variant of this command to reset quiet period to the default (60 seconds).

**Syntax** `auth timeout quiet-period <1-65535>`  
`no auth timeout quiet-period`

| Parameter   | Description |
|-------------|-------------|
| <1 - 65535> | Seconds.    |

**Default** The quiet period of port authentication is 60 seconds.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To set the quiet period to 10 for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout quiet-period 10
```

To reset the quiet period to the default (60 seconds) for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout quiet-period
```



# auth timeout reauth-period

**Overview** This command sets the timer for reauthentication on a given interface. The re-authentication for the supplicant (client device) is executed at this timeout. The timeout is only applied if the **auth reauthentication** command is applied.

Use the **no** variant of this command to reset the **reauth-period** parameter to the default (3600 seconds).

**Syntax** `auth timeout reauth-period <1-4294967295>`  
`no auth timeout reauth-period`

| Parameter      | Description |
|----------------|-------------|
| <1-4294967295> | Seconds.    |

**Default** The default reauthentication period for port authentication is 3600 seconds, when reauthentication is enabled on the port.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To set the reauthentication period to 1 day for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout reauth-period 86400
```

To reset the reauthentication period to the default (3600 seconds) for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout reauth-period
```

**Validation Commands** `show dot1x`  
`show dot1x interface`  
`show running-config`

**Related Commands** `auth reauthentication`

# auth timeout server-timeout

**Overview** This command sets the timeout for the waiting response from the RADIUS server on a given interface.

The **no** variant of this command resets the server-timeout to the default (30 seconds).

**Syntax** `auth timeout server-timeout <1-65535>`  
`no auth timeout server-timeout`

| Parameter | Description |
|-----------|-------------|
| <1-65535> | Seconds.    |

**Default** The server timeout for port authentication is 30 seconds.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To set the server timeout to 120 seconds for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout server-timeout 120
```

To set the server timeout to the default (30 seconds) for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout server-timeout
```

**Validation  
Commands** `show dot1x`  
`show dot1x interface`  
`show running-config`

# auth timeout supp-timeout

**Overview** This command sets the timeout of the waiting response from the supplicant (client device) on a given interface.

The **no** variant of this command resets the supplicant timeout to the default (30 seconds).

**Syntax** `auth timeout supp-timeout <1-65535>`  
`no auth timeout supp-timeout`

| Parameter | Description |
|-----------|-------------|
| <1-65535> | Seconds.    |

**Default** The supplicant timeout of port authentication is 30 seconds.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To set the server timeout to 2 seconds for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout supp-timeout 2
```

To reset the server timeout to the default (30 seconds) for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout supp-timeout
```

**Validation Commands** `show dot1x`  
`show dot1x interface`  
`show running-config`

# auth two-step enable

**Overview** This command enables a two-step authentication feature on an interface. When this feature is enabled, the supplicant is authorized in a two-step process. If authentication succeeds, the supplicant becomes authenticated. This command will apply the two-step authentication method based on 802.1X-, MAC- or Web-Authentication.

The **no** variant of this command disables the two-step authentication feature.

**Syntax** auth two-step enable  
no auth two-step enable

**Default** Default.

**Mode** Interface Configuration for a port.

**Usage** The single step authentication methods (either user or device authentication) have a potential security risk:

- an unauthorized user can access the network with an authorized device, or
- an authorized user can access the network with an unauthorized device.

Two-step authentication solves this problem by authenticating both the user and the device. The supplicant will only become authenticated if both these steps are successful. If the first authentication step fails, then the second step is not started.

**Examples** To enable the two step authentication feature, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth two-step enable
```

To disable the two step authentication feature, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth two-step enable
```

To enable MAC-Authentication followed by 802.1X-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

To enable MAC-Authentication followed by Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

To enable 802.1X-Authentication followed by Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-web enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

**Validation  
Commands**

- show startup-config
- show auth-mac supplicant
- show dot1x supplicant

**Related  
Commands**

- show auth two-step supplicant brief
- show auth-mac
- show auth-mac interface
- show auth-mac supplicant
- show auth-web
- show auth-web interface
- show auth-web supplicant
- show dot1x
- show dot1x interface
- show dot1x supplicant

# auth-mac enable

**Overview** This command enables MAC-based authentication on the interface specified in the Interface command mode.

Use the **no** variant of this command to disable MAC-based authentication on an interface.

**Syntax** auth-mac enable  
no auth-mac enable

**Default** MAC-Authentication is disabled by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** Enabling **spanning-tree edgeport** on ports after enabling MAC-based authentication avoids unnecessary re-authentication when the port state changes, which does not happen when spanning tree edgeport is enabled. Note that re-authentication is correct behavior without **spanning-tree edgeport** enabled.

Applying **switchport mode access** on ports is also good practice to set the ports to access mode with ingress filtering turned on, whenever ports for MAC-Authentication are in a VLAN.

**Examples** To enable MAC-Authentication on interface port1.0.2 and enable spanning tree edgeport to avoid unnecessary re-authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac enable
awplus(config-if)# spanning-tree edgeport
awplus(config-if)# switchport mode access
```

To disable MAC-Authentication on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-mac enable
```

**Validation Commands** show auth-mac  
show auth-mac interface  
show running-config

**Related  
Commands**    [aaa accounting auth-mac default](#)  
[aaa authentication auth-mac](#)  
[spanning-tree edgeport \(RSTP and MSTP\)](#)  
[switchport mode access](#)



# auth-mac method

**Overview** This command sets the type of authentication method for MAC-Authentication that is used with RADIUS on the interface specified in the Interface command mode.

The **no** variant of this command resets the authentication method used to the default method (PAP) as the RADIUS authentication method used by the MAC-Authentication.

**Syntax** `auth-mac method [eap-md5|pap]`  
`no auth-mac method`

| Parameter | Description                              |
|-----------|------------------------------------------|
| eap-md5   | Enable EAP-MD5 of authentication method. |
| pap       | Enable PAP of authentication method.     |

**Default** The MAC-Authentication method is PAP.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To set the MAC-Authentication method to pap on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac method pap
```

To set the MAC-Authentication method to the default on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-mac method
```

**Validation  
Commands** `show auth-mac`  
`show auth-mac interface`  
`show running-config`

# auth-mac password

**Overview** This command changes the password for MAC-based authentication.  
Use the **no** variant of this command to return the password to its default.

**Syntax** auth-mac [encrypted] password <password>  
no auth-mac password

| Parameter  | Description                                                                                                                                                                                                      |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auth-mac   | MAC-based authentication                                                                                                                                                                                         |
| encrypted  | Specify an encrypted password                                                                                                                                                                                    |
| password   | Configure the password                                                                                                                                                                                           |
| <password> | The new password. Passwords can be up to 64 characters in length and can contain any printable characters except <ul style="list-style-type: none"><li>• ?</li><li>• " (double quotes)</li><li>• space</li></ul> |

**Default** By default, the password is the MAC address of the supplicant

**Mode** Global Configuration

**Usage** Changing the password increases the security of MAC-based authentication, because the default password is easy for an attacker to discover. This is particularly important if:

- some MAC-based supplicants on the network are intelligent devices, such as computers, and/or
- you are using two-step authentication (see the “Ensuring Authentication Methods Require Different Usernames and Passwords” section of the [Authentication Feature Overview and Configuration Guide](#)).

**Examples** To change the password to verySecurePassword, use the commands:

```
awplus# configure terminal
awplus(config)# auth-mac password verySecurePassword
```

**Validation Command** [show running-config](#)

**Related Commands** [auth two-step enable](#)  
[show auth-mac](#)

# auth-mac reauth-relearning

**Overview** This command sets the MAC address learning of the supplicant (client device) to re-learning for re-authentication on the interface specified in the Interface command mode.

Use the **no** variant of this command to disable the auth-mac re-learning option.

**Syntax** auth-mac reauth-relearning  
no auth-mac reauth-relearning

**Default** Re-learning for port authentication is disabled by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To enable the re-authentication re-learning feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac reauth-relearning
```

To disable the re-authentication re-learning feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-mac reauth-relearning
```

**Validation  
Commands** show auth-mac  
show auth-mac interface  
show running-config

# auth-web enable

**Overview** This command enables Web-based authentication in Interface mode on the interface specified.

Use the **no** variant of this command to disable Web-based authentication on an interface.

**Syntax** auth-web enable  
no auth-web enable

**Default** Web-Authentication is disabled by default.

**Mode** Interface Configuration for a static channel or a switch port.

**Usage** Web-based authentication cannot be enabled if DHCP snooping is enabled by using the [service dhcp-snooping](#) command, and vice versa. You need to configure an IPv4 address for the VLAN interface on which Web Authentication is running.

**Examples** To enable Web-Authentication on static-channel-group 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)# auth-web enable
```

To disable Web-Authentication on static-channel-group 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)# no auth-web enable
```

**Validation Commands** [show auth-web](#)  
[show auth-web interface](#)  
[show running-config](#)

**Related Commands** [aaa accounting auth-web default](#)  
[aaa authentication auth-web](#)

# auth-web forward

**Overview** This command enables the Web-Authentication packet forwarding feature on the interface specified. This command also enables ARP forwarding, and adds forwarded packets to the **tcp** or **udp** port number specified.

The **no** variant of this command disables or deletes the packet forwarding feature on the interface.

**Syntax** `auth-web forward [<ip-address>] {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}`  
`no auth-web forward [<ip-address>] {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}`

| Parameter    | Description                                        |
|--------------|----------------------------------------------------|
| <ip-address> | Enable forwarding to the destination IPv4 address. |
| arp          | Enable forwarding of ARP.                          |
| dhcp         | Enable forwarding of DHCP (67/udp).                |
| dns          | Enable forwarding of DNS (53/udp).                 |
| tcp          | Enable forwarding of TCP specified port number.    |
| <1-65535>    | TCP Port number.                                   |
| udp          | Enable forwarding of UDP specified port number.    |
| <1-65535>    | UDP Port number.                                   |

**Default** Packet forwarding for port authentication is disabled by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Usage** For more information about the <ip-address> parameter, and an example, see the "auth- web forward" section in the [Alliedware Plus Technical Tips and Tricks](#).

**Examples** To enable the ARP forwarding feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web forward arp
```

To add the TCP forwarding port 137 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web forward tcp 137
```

To add the DNS Server IP address 192.168.1.10 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth-web forward 192.168.1.10 dns
```

To disable the ARP forwarding feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward arp
```

To delete the TCP forwarding port 137 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward tcp 137
```

To delete the all of TCP forwarding on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward tcp
```

**Validation  
Commands**

- [show auth-web](#)
- [show auth-web interface](#)
- [show running-config](#)

# auth-web max-auth-fail

**Overview** This command sets the number of authentication failures allowed before rejecting further authentication requests. When the supplicant (client device) fails more than has been set to the maximum number of authentication failures then login requests are refused during the quiet period.

The **no** variant of this command resets the maximum number of authentication failures to the default (three authentication failures).

**Syntax** `auth-web max-auth-fail <0-10>`  
`no auth-web max-auth-fail`

| Parameter                 | Description           |
|---------------------------|-----------------------|
| <code>&lt;0-10&gt;</code> | Lock count specified. |

**Default** The **max-auth-fail** lock counter is set to three authentication failures by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Examples** To set the lock count to 5 on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web max-auth-fail 5
```

To set the lock count to the default on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web max-auth-fail
```

**Validation Commands** `show auth-web`  
`show auth-web interface`  
`show running-config`

**Related Commands** `auth timeout quiet-period`

# auth-web method

**Overview** This command sets the authentication method of Web-Authentication that is used with RADIUS on the interface specified.

The **no** variant of this command sets the authentication method to PAP for the interface specified when Web-Authentication is also used with the RADIUS authentication method.

**Syntax** `auth-web method {eap-md5|pap}`  
`no auth-web method`

| Parameter | Description                                  |
|-----------|----------------------------------------------|
| eap-md5   | Enable EAP-MD5 as the authentication method. |
| pap       | Enable PAP as the authentication method.     |

**Default** The Web-Authentication method is set to PAP by default.

**Mode** Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

**Example** To set the Web-Authentication method to eap-md5 on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web method eap-md5
```

**Validation Commands** `show auth-web`  
`show auth-web interface`  
`show running-config`



# auth-web-server blocking-mode

**Overview** Use this command to enable blocking mode for the Web-Authentication server. The blocking mode displays an authentication success or failure screen immediately from the response result from a RADIUS server.

Use the **no** variant of this command to disable blocking mode for the Web-Authentication server.

**Syntax** `auth-web-server blocking-mode`  
`no auth-web-server blocking-mode`

| Parameter                  | Description                                 |
|----------------------------|---------------------------------------------|
| <code>blocking-mode</code> | Use blocking authentication server process. |
| <code>no</code>            | Disable blocking mode.                      |

**Default** By default, blocking mode is disabled for the Web-Authentication server.

**Mode** Global Configuration

**Example** To enable blocking mode for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server blocking-mode
```

To disable blocking mode for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server blocking-mode
```

**Validation Commands** `show running-config`

**Related Commands** `show auth-web-server`  
`auth-web-server mode (deleted)`  
`auth-web-server redirect-delay-time`

# auth-web-server dhcp ipaddress

**Overview** Use this command to assign an IP address and enable the DHCP service on the Web-Authentication server for supplicants (client devices).

Use the **no** variant of this command to remove an IP address and disable the DHCP service on the Web-Authentication server for supplicants.

**Syntax** `auth-web-server dhcp ipaddress <ip-address/prefix-length>`  
`no auth-web-server dhcp ipaddress`

| Parameter                                  | Description                                                                                                        |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ip-addr/prefix-length&gt;</code> | The IPv4 address and prefix length assigned for the DHCP service on the Web-Authentication server for supplicants. |

**Default** No IP address for the Web-Authentication server is set by default.

**Mode** Global Configuration

**Usage** See the [Authentication Feature Overview and Configuration Guide](#) for information about:

- using DHCP with web authentication, and
- restrictions regarding combinations of authentication enhancements working together

**Examples** To assign the IP address 10.0.0.1 to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp ipaddress 10.0.0.1/8
```

To remove an IP address on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp ipaddress
```

**Validation Commands** [show running-config](#)

**Related Commands** [show auth-web-server](#)  
[auth-web-server dhcp lease](#)

# auth-web-server dhcp lease

**Overview** Use this command to set the DHCP lease time for supplicants (client devices) using the DHCP service on the Web-Authentication server.

Use the **no** variant of this command to reset to the default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server.

**Syntax** auth-web-server dhcp lease <20-60>  
no auth-web-server dhcp lease

| Parameter | Description                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------|
| <20-60>   | DHCP lease time for supplicants using the DHCP service on the Web-Authentication server in seconds. |

**Default** The default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server is set to 30 seconds.

**Mode** Global Configuration

**Usage** See the [Authentication Feature Overview and Configuration Guide](#) for information about:

- using DHCP with web authentication, and
- restrictions regarding combinations of authentication enhancements working together

**Examples** To set the DHCP lease time to 1 minute for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp lease 60
```

To reset the DHCP lease time to the default setting (30 seconds) for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp lease
```

**Validation Commands** [show running-config](#)

**Related Commands** [show auth-web-server](#)  
[auth-web-server dhcp ipaddress](#)

# auth-web-server dhcp-wpad-option

**Overview** This command sets the DHCP WPAD (Web Proxy Auto-Discovery) option for the Web-Authentication temporary DHCP service.

For more information and examples, see the “Web Auth Proxy” section in the [Alliedware Plus Technical Tips and Tricks](#).

Use the **no** variant of this command to disable the DHCP WPAD function.

**Syntax** `auth-web-server dhcp wpad-option <url>`  
`no auth-web-server dhcp wpad-option`

| Parameter | Description                               |
|-----------|-------------------------------------------|
| <url>     | URL to the server which gets a .pac file. |

**Default** The Web-Authentication server DHCP WPAD option is not set.

**Mode** Global Configuration

**Usage** If the supplicant is configured to use WPAD, the supplicant’s web browser will use TCP port 80 as usual. Therefore, the packet can be intercepted by Web-Authentication as normal, and the Web-Authentication Login page can be sent. However, after authentication, the browser does not know where to get the WPAD file and so cannot access external web pages. The WPAD file is usually named proxy.pac file and tells the browser what web proxy to use.

Use this command to tell the supplicant where it can get this file from. The switch itself can be specified as the source for this file, and it can deliver it to the supplicant on request.

**Example** To specify that the proxy.pac file is found on the server at 192.168.1.100, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp wpad-option
http://192.168.1.100/proxy/proxy.pac
```

**Related Commands** [show auth-web-server](#)

# auth-web-server gateway (deleted)

**Overview** This command has been deleted.

# auth-web-server host-name

**Overview** This command assigns a hostname to the web authentication server.

Use the **no** variant of this command to remove the hostname from the web authentication server.

**Syntax** `auth-web-server host-name <hostname>`  
`no auth-web-server host-name`

| Parameter                     | Description                |
|-------------------------------|----------------------------|
| <code>&lt;hostname&gt;</code> | URL string of the hostname |

**Default** The web authentication server has no hostname.

**Mode** Global Configuration

**Usage** When the web authentication server uses HTTPS protocol, the web browser will validate the certificate. If the certificate is invalid, the web page gives a warning message before displaying server content. However, the web page will not give warning message if the server has a hostname same as the one stored in the installed certificate.

**Examples** To set the auth.example.com as the hostname of the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server host-name auth.example.com
```

To remove hostname auth.example.com from the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server host-name
```

**Related Commands** [aaa authentication auth-web](#)  
[auth-web enable](#)

# auth-web-server http-redirect (deleted)

**Overview** This command has been deleted.

# auth-web-server intercept-port

**Overview** This command specifies any additional TCP port numbers that the Web-Authentication server is to intercept.

Use the **no** variant of this command to stop intercepting the TCP port numbers.

**Syntax** `auth-web-server intercept-port <1-65535>`  
`no auth-web-server intercept-port <1-65535>`

| Parameter   | Description      |
|-------------|------------------|
| <1 - 65535> | TCP port number. |

**Default** No additional TCP port numbers are intercepted by default.

**Mode** Global Configuration

**Usage** If this command is not specified, AlliedWare Plus Web-Authentication intercepts the supplicant's initial TCP port 80 connection to a web page and sends it the Web-Authentication Login page. However, if the supplicant is configured to use a web proxy, then it will usually be using TCP port 8080 (or another user configured port number). In this case Web-Authentication cannot intercept the connection.

To overcome this limitation you can now use this command to tell the switch which additional port it should intercept, and then send the Web-Authentication Login page to the supplicant.

When you use this command in conjunction with a proxy server configured in the web browser, you must add the proxy server's network as a 'No Proxy' network. You can specify 'No Proxy' networks in the proxy settings in your web browser. For more information, see the "Web Auth Proxy" section in the [Alliedware Plus Technical Tips and Tricks](#).

**Example** To additionally intercept port number 3128, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server intercept-port 3128
```

**Related Commands** [show auth-web-server](#)



# auth-web-server ipaddress

**Overview** This command sets the IP address for the Web-Authentication server.  
Use the **no** variant of this command to delete the IP address for the Web-Authentication server.

**Syntax** `auth-web-server ipaddress <ip-address>`  
`no auth-web-server ipaddress`

| Parameter                       | Description                                                            |
|---------------------------------|------------------------------------------------------------------------|
| <code>&lt;ip-address&gt;</code> | Web-Authentication server dotted decimal IP address in A.B.C.D format. |

**Default** The Web-Authentication server address on the system is not set by default.

**Mode** Global Configuration

**Examples** To set the IP address 10.0.0.1 to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# auth-web-server ipaddress 10.0.0.1
```

To delete the IP address from the Web-Authentication server, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no auth-web-server ipaddress
```

**Validation Commands** `show auth-web`  
`show auth-web-server`  
`show running-config`

# auth-web-server login-url

**Overview** This command sets the web-authentication login page URL.  
Use the **no** variant of this command to delete the set URL.

**Syntax** `auth-web-server login-url <URL>`  
`no auth-web-server login-url`

| Parameter | Description        |
|-----------|--------------------|
| <URL>     | Set login page URL |

**Default** The built-in login page is set by default.

**Mode** Global Configuration

**Examples** To set `http://example.com/login.html` as the login page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server login-url
http://example.com/login.html
```

To unset the login page URL, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server login-url
```

**Validation  
Commands** **show running-config**

# auth-web-server mode (deleted)

**Overview** This command has been deleted.

# auth-web-server page logo

**Overview** This command sets the type of logo that will be displayed on the web authentication page.

Use the **no** variant of this command to set the logo type to **auto**.

**Syntax** `auth-web-server page logo {auto|default|hidden}`  
`no auth-web-server page logo`

| Parameter | Description                                                              |
|-----------|--------------------------------------------------------------------------|
| auto      | Display the custom logo if installed; otherwise display the default logo |
| default   | Display the default logo                                                 |
| hidden    | Hide the logo                                                            |

**Default** Logo type is **auto** by default.

**Mode** Global Configuration

**Examples** To display the default logo with ignoring installed custom logo, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page logo default
```

To set back to the default logo type **auto**, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page logo
```

**Validation Commands** `show auth-web-server page`

# auth-web-server page sub-title

**Overview** This command sets the custom sub-title on the web authentication page.  
Use the **no** variant of this command to reset the sub-title to its default.

**Syntax** `auth-web-server page sub-title {hidden|text <sub-title>}`  
`no auth-web-server page sub-title`

| Parameter   | Description                  |
|-------------|------------------------------|
| hidden      | Hide the sub-title           |
| <sub-title> | Text string of the sub-title |

**Default** "Allied-Telesis" is displayed by default.

**Mode** Global Configuration

**Examples** To set the custom sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title text Web
Authentication
```

To hide the sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title hidden
```

To change back to the default title, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page sub-title
```

**Validation  
Commands** [show auth-web-server page](#)

# auth-web-server page success-message

**Overview** This command sets the success message on the web-authentication page.

Use the **no** variant of this command to remove the success message.

**Syntax** auth-web-server page success-message text *<success-message>*  
no auth-web-server page success-message

| Parameter                      | Description                        |
|--------------------------------|------------------------------------|
| <i>&lt;success-message&gt;</i> | Text string of the success message |

**Default** No success message is set by default.

**Mode** Global Configuration

**Examples** To set the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# auth-web-server page success-message text Your
success message
```

To unset the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no auth-web-server page success-message
```

**Validation  
Commands** show auth-web-server page

# auth-web-server page title

**Overview** This command sets the custom title on the web authentication page.  
Use the **no** variant of this command to remove the custom title.

**Syntax** auth-web-server page title {hidden|text <title>}  
no auth-web-server page title

| Parameter | Description              |
|-----------|--------------------------|
| hidden    | Hide the title           |
| <title>   | Text string of the title |

**Default** "Web Access Authentication Gateway" is displayed by default.

**Mode** Global Configuration

**Examples** To set the custom title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page title text Login
```

To hide the title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page title hidden
```

To unset the custom title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page title
```

**Validation  
Commands** [show auth-web-server page](#)

# auth-web-server page welcome-message

**Overview** This command sets the welcome message on the web-authentication page.  
Use the **no** variant of this command to remove the welcome message.

**Syntax** auth-web-server page welcome-message text *<welcome-message>*  
no auth-web-server page welcome-message

| Parameter                      | Description                        |
|--------------------------------|------------------------------------|
| <i>&lt;welcome-message&gt;</i> | Text string of the welcome message |

**Default** No welcome message is set by default.

**Mode** Global Configuration

**Examples** To set the welcome message on the web-authentication page, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# auth-web-server page welcome-message text Your
welcome message
```

To remove the welcome message on the web-authentication page, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no auth-web-server page welcome-message
```

**Validation  
Commands** [show auth-web-server page](#)



# auth-web-server ping-poll enable

**Overview** This command enables the ping polling to the supplicant (client device) that is authenticated by Web-Authentication.

The **no** variant of this command disables the ping polling to the supplicant that is authenticated by Web-Authentication.

**Syntax** auth-web-server ping-poll enable  
no auth-web-server ping-poll enable

**Default** The ping polling feature for Web-Authentication is disabled by default.

**Mode** Global Configuration

**Examples** To enable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll enable
```

To disable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll enable
```

**Validation  
Commands** show auth-web  
show auth-web-server  
show running-config

# auth-web-server ping-poll failcount

**Overview** This command sets a fail count for the ping polling feature when used with Web-Authentication. The **failcount** parameter specifies the number of unanswered pings. A supplicant (client device) is logged off when the number of unanswered pings are greater than the failcount set with this command.

Use the **no** variant of this command to resets the fail count for the ping polling feature to the default (5 pings).

**Syntax** `auth-web-server ping-poll failcount <1-100>`  
`no auth-web-server ping-poll failcount`

| Parameter | Description |
|-----------|-------------|
| <1-100>   | Count.      |

**Default** The default failcount for ping polling is 5 pings.

**Mode** Global Configuration

**Examples** To set the failcount of ping polling to 10 pings, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll failcount 10
```

To set the failcount of ping polling to default, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll failcount
```

**Validation  
Commands** `show auth-web`  
`show auth-web-server`  
`show running-config`

# auth-web-server ping-poll interval

**Overview** This command is used to change the ping poll interval. The interval specifies the time period between pings when the supplicant (client device) is reachable.

Use the **no** variant of this command to reset to the default period for ping polling (30 seconds).

**Syntax** `auth-web-server ping-poll interval <1-65535>`  
`no auth-web-server ping-poll interval`

| Parameter | Description |
|-----------|-------------|
| <1-65535> | Seconds.    |

**Default** The interval for ping polling is 30 seconds by default.

**Mode** Global Configuration

**Examples** To set the interval of ping polling to 60 seconds, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# auth-web-server ping-poll interval 60
```

To set the interval of ping polling to the default (30 seconds), use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no auth-web-server ping-poll interval
```

**Validation  
Commands** `show auth-web`  
`show auth-web-server`  
`show running-config`

# auth-web-server ping-poll reauth-timer-refresh

**Overview** This command modifies the **reauth-timer-refresh** parameter for the Web-Authentication feature. The **reauth-timer-refresh** parameter specifies whether a re-authentication timer is reset and when the response from a supplicant (a client device) is received.

Use the **no** variant of this command to reset the **reauth-timer-refresh** parameter to the default setting (disabled).

**Syntax** auth-web-server ping-poll reauth-timer-refresh  
no auth-web-server ping-poll reauth-timer-refresh

**Default** The reauth-timer-refresh parameter is disabled by default.

**Mode** Global Configuration

**Examples** To enable the reauth-timer-refresh timer, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll reauth-timer-refresh
```

To disable the reauth-timer-refresh timer, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll
reauth-timer-refresh
```

**Validation  
Commands** show auth-web  
show auth-web-server  
show running-config

# auth-web-server ping-poll timeout

**Overview** This command modifies the ping poll **timeout** parameter for the Web-Authentication feature. The **timeout** parameter specifies the time in seconds to wait for a response to a ping packet.

Use the **no** variant of this command to reset the timeout of ping polling to the default (1 second).

**Syntax** `auth-web-server ping-poll timeout <1-30>`  
`no auth-web-server ping-poll timeout`

| Parameter | Description |
|-----------|-------------|
| <1 - 30>  | Seconds.    |

**Default** The default timeout for ping polling is 1 second.

**Mode** Global Configuration

**Examples** To set the timeout of ping polling to 2 seconds, use the command:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll timeout 2
```

To set the timeout of ping polling to the default (1 second), use the command:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll timeout
```

**Validation  
Commands** `show auth-web`  
`show auth-web-server`  
`show running-config`

# auth-web-server port

**Overview** This command sets the HTTP port number for the Web-Authentication server. Use the **no** variant of this command to reset the HTTP port number to the default (80).

**Syntax** `auth-web-server port <port-number>`  
`no auth-web-server port`

| Parameter                        | Description                                                                               |
|----------------------------------|-------------------------------------------------------------------------------------------|
| <code>&lt;port-number&gt;</code> | Set the local Web-Authentication server port within the TCP port number range 1 to 65535. |

**Default** The Web-Authentication server HTTP port number is set to 80 by default.

**Mode** Global Configuration

**Examples** To set the HTTP port number 8080 for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server port 8080
```

To reset to the default HTTP port number 80 for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server port
```

**Validation Commands** `show auth-web`  
`show auth-web-server`  
`show running-config`

# auth-web-server redirect-delay-time

**Overview** Use this command to set the delay time in seconds before redirecting the supplicant to a specified URL when the supplicant is authorized.

Use the variant **no** to reset the delay time set previously.

**Syntax** `auth-web-server redirect-delay-time <5-60>`  
`no auth-web-server redirect-delay-time`

| Parameter                        | Description                                                                              |
|----------------------------------|------------------------------------------------------------------------------------------|
| <code>redirect-delay-time</code> | Set the delay time before jumping to a specified URL after the supplicant is authorized. |
| <code>&lt;5-60&gt;</code>        | The time in seconds.                                                                     |

**Default** The default redirect delay time is 5 seconds.

**Mode** Global Configuration

**Examples** To set the delay time to 60 seconds for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-delay-time 60
```

To reset the delay time, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-delay-time
```

**Validation Command** `show auth-web-servers``show running-config`

**Related Commands** `auth-web-server redirect-url`  
`show auth-web-server`  
`auth-web-server blocking-mode`

# auth-web-server redirect-url

**Overview** This command sets a URL for supplicant (client device) authentication. When a supplicant is authorized it will be automatically redirected to the specified URL. Note that if the http redirect feature is used then this command is ignored.

Use the **no** variant of this command to delete the URL string set previously.

**Syntax** `auth-web-server redirect-url <url>`  
`no auth-web-server redirect-url`

| Parameter                | Description                           |
|--------------------------|---------------------------------------|
| <code>&lt;url&gt;</code> | URL (hostname or dotted IP notation). |

**Default** The redirect URL for the Web-Authentication server feature is not set by default (null).

**Mode** Global Configuration

**Examples** To enable and set redirect a URL string `www.alliedtelesis.com` for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-url
http://www.alliedtelesis.com
```

To delete a redirect URL string, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-url
```

**Validation  
Commands** `show auth-web`  
`show auth-web-server`  
`show running-config`

**Related  
Commands** `auth-web-server http-redirect (deleted)`  
`auth-web-server redirect-delay-time`



# auth-web-server session-keep

**Overview** This command enables the session-keep feature to jump to the original URL after being authorized by Web-Authentication.

Use the **no** variant of this command to disable the session keep feature.

**Syntax** `auth-web-server session-keep`  
`no auth-web-server session-keep`

**Default** The session-keep feature is disabled by default.

**Mode** Global Configuration

**Usage** This function doesn't ensure to keep session information in all cases. Authenticated supplicant may be redirected to unexpected page when session-keep is enabled. This issue occurred by supplicant sending HTTP packets automatically after authentication page is displayed and the URL is written.

**Examples** To enable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server session-keep
```

To disable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server session-keep
```

**Validation  
Commands** `show auth-web`  
`show auth-web-server`  
`show running-config`

# auth-web-server ssl

**Overview** This command enables HTTPS functionality for the Web-Authentication server feature.

Use the **no** variant of this command to disable HTTPS functionality for the Web-Authentication server.

**Syntax** auth-web-server ssl  
no auth-web-server ssl

**Default** HTTPS functionality for the Web-Authentication server feature is disabled by default.

**Mode** Global Configuration

**Examples** To enable HTTPS functionality for the Web-Authentication server feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ssl
```

To disable HTTPS functionality for the Web-Authentication server feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ssl
```

**Validation  
Commands** show auth-web  
show auth-web-server  
show running-config

# auth-web-server sslport (deleted)

**Overview** This command has been deleted.

# auth-web-server ssl intercept-port

**Overview** Use this command to register HTTPS intercept port numbers when the HTTPS server uses custom port number (not TCP port number 443).

Note that you need to use the **auth-web-server intercept-port** command to register HTTP intercept port numbers.

Use the **no** variant of this command to delete registered port number.

**Syntax** `auth-web-server ssl intercept-port <1-65535>`  
`no auth-web-server ssl intercept-port <1-65535>`

| Parameter | Description                                       |
|-----------|---------------------------------------------------|
| <1-65535> | TCP port number in the range from 1 through 65535 |

**Default** 443/TCP is registered by default.

**Mode** Global Configuration

**Examples** To register HTTPS port number 3128, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ssl intercept-port 3128
```

To delete HTTPS port number 3128, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ssl intercept-port 3128
```

**Validation Commands** `show auth-web-server`

**Related Commands** `auth-web-server intercept-port`

# copy proxy-autoconfig-file

**Overview** Use this command to download the proxy auto configuration (PAC) file to your switch. The Web-Authentication supplicant can get the downloaded file from the system web server.

**Syntax** `copy <filename> proxy-autoconfig-file`

| Parameter  | Description              |
|------------|--------------------------|
| <filename> | The URL of the PAC file. |

**Mode** Privileged Exec

**Example** To download the PAC file to this device, use the command:  
`awplus# copy tftp://server/proxy.pac proxy-autoconfig-file`

**Related Commands** [show proxy-autoconfig-file](#)  
[erase proxy-autoconfig-file](#)

## copy web-auth-https-file

**Overview** Use this command to download the SSL server certificate for web-based authentication. The file must be in PEM (Privacy Enhanced Mail) format, and contain the private key and the server certificate.

**Syntax** `copy <filename> web-auth-https-file`

| Parameter  | Description                             |
|------------|-----------------------------------------|
| <filename> | The URL of the server certificate file. |

**Mode** Privileged Exec

**Example** To download the server certificate file `verisign_cert.pem` from the TFTP server directory `server`, use the command:

```
awplus# copy tftp://server/verisign_cert.pem
web-auth-https-file
```

**Related Commands**

- [auth-web-server ssl](#)
- [erase web-auth-https-file](#)
- [show auth-web-server](#)

# erase proxy-autoconfig-file

**Overview** Use this command to remove the proxy auto configuration file.

**Syntax** erase proxy-autoconfig-file

**Mode** Privileged Exec

**Example** To remove the proxy auto configuration file, use the command:

```
awplus# erase proxy-autoconfig-file
```

**Related  
Commands** [show proxy-autoconfig-file](#)  
[copy proxy-autoconfig-file](#)

# erase web-auth-https-file

**Overview** Use this command to remove the SSL server certificate for web-based authentication.

**Syntax** erase web-auth-https-file

**Mode** Privileged Exec

**Example** To remove the SSL server certificate file for web-based authentication use the command:

```
awplus# erase web-auth-https-file
```

**Related  
Commands**

- [auth-web-server ssl](#)
- [copy web-auth-https-file](#)
- [show auth-web-server](#)



# show auth two-step supplicant brief

**Overview** This command displays the supplicant state of the two-step authentication feature on the interface.

**Syntax** show auth two-step supplicant [interface <ifrange>] brief

| Parameter | Description                                                                                                                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface | The interface selected for display.                                                                                                                                                                                                |
| <ifrange> | The interface types which can be specified as <ifrange> <ul style="list-style-type: none"><li>• Switch port (e.g. port1.0.6)</li><li>• Static channel group (e.g. sa3)</li><li>• Dynamic (LACP) channel group (e.g. po4)</li></ul> |

**Mode** Privileged Exec

**Usage** Do not mix interface types in a list. The specified interfaces must exist.

**Example** To display the supplicant state of the two-step authentication feature, enter the command:

```
awplus# show two-step supplicant interface port1.0.6 brief
```

**Output** Figure 28-1: Example output from the **show auth two-step** supplicant brief command

```
interface port1.0.6

authenticationMethod: dot1x/mac

Two-Step Authentication:
 firstMethod:mac
 secondMethod:dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
 macBasedAuthenticationSupplicantNum: 0
 dot1xAuthenticationSupplicantNum: 1
 webBasedAuthenticationSupplicantNum: 0
 otherAuthenticationSupplicantNum: 0

Interface VID Mode MAC Address Status FirstStep SecondStep
===== === === =====
port1.0.6
 1 D 000b..db67.00f7 Authenticated Pass Pass
```

**Related Commands** [auth two-step enable](#)

# show auth-mac

**Overview** This command shows authentication information for MAC-based authentication.

**Syntax** show auth-mac [all]

| Parameter | Description                                                                        |
|-----------|------------------------------------------------------------------------------------|
| all       | Display all authentication information for each interface available on the switch. |

**Mode** Privileged Exec

**Example** To display all MAC-based authentication information, enter the command:

```
awplus# show auth-mac all
```

**Output** Figure 28-2: Example output from the **show auth-mac** command

```
802.1X Port-Based Authentication Disabled
MAC-based Port Authentication Enabled
WEB-based Port Authentication Disabled
```

**Related  
Commands** [show dot1x](#)  
[show auth-web](#)

## show auth-mac diagnostics

**Overview** This command shows MAC-Authentication diagnostics, optionally for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

**Syntax** show auth-mac diagnostics [interface <interface-list>]

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface        | Specify an interface to show                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <interface-list> | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• an interface (e.g. vlan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. vlan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |

**Mode** Privileged Exec

**Example** To display authentication diagnostics for port1.0.6, enter the command:

```
awplus# show auth-mac diagnostics interface port1.0.6
```

**Output** Figure 28-3: Example output from the **show auth-mac diagnostics** command

```
Authentication Diagnostics for interface port1.0.6
 Supplicant address: 00d0.59ab.7037
 authEnterConnecting: 2
 authEaplogoffWhileConnecting: 1
 authEnterAuthenticating: 2
 authSuccessWhileAuthenticating: 1
 authTimeoutWhileAuthenticating: 1
 authFailWhileAuthenticating: 0
 authEapstartWhileAuthenticating: 0
 authEaplogoggWhileAuthenticating: 0
 authReauthsWhileAuthenticated: 0
 authEapstartWhileAuthenticated: 0
 authEaplogoffWhileAuthenticated: 0
 BackendResponses: 2
 BackendAccessChallenges: 1
 BackendOtherrequestToSupplicant: 3
 BackendAuthSuccess: 1
```

# show auth-mac interface

**Overview** This command shows the status for MAC-based authentication on the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interface. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interface. Use the optional **statistics** parameter to show authentication diagnostics for the specified interface. Use the optional **supplicant**(client device) parameter to show the supplicant state for the specified interface.

**Syntax** show auth-mac interface <interface-list>  
[diagnostics|sessionstatistics|statistics|supplicant [brief]]

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface-list>  | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• an interface (e.g. v lan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v lan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |
| diagnostics       | Diagnostics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| sessionstatistics | Session statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| statistics        | Statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| supplicant        | Supplicant (client device).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| brief             | Brief summary of supplicant state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

**Mode** Privileged Exec

**Examples** To display MAC-based authentication status for port1.0.2, enter the command:  
awplus# show auth-mac interface port1.0.2

```
% Port-Control not configured on port1.0.2
```

To display MAC-Authentication diagnostics for port1.0.2, enter the command:

```
awplus# show auth-mac interface port1.0.2 diagnostics
```

```
Authentication Diagnostics for interface port1.0.2
 Supplicant address: 00d0.59ab.7037
 authEnterConnecting: 2
 authEaplogoffWhileConnecting: 1
 authEnterAuthenticating: 2
 authSuccessWhileAuthenticating: 1
 authTimeoutWhileAuthenticating: 1
 authFailWhileAuthenticating: 0
 authEapstartWhileAuthenticating: 0
 authEaplogoggWhileAuthenticating: 0
 authReauthsWhileAuthenticated: 0
 authEapstartWhileAuthenticated: 0
 authEaplogoffWhileAuthenticated: 0
 BackendResponses: 2
 BackendAccessChallenges: 1
 BackendOtherrequestToSupplicant: 3
 BackendAuthSuccess: 1
```

To display authentication session statistics for port1.0.6, enter the command:

```
awplus# show auth-mac interface port1.0.6 sessionstatistics
```

```
Authentication
session statistics for interface port1.0.6
 session user name: manager
 session authentication method: Remote server
 session time: 19440 secs
 session terminat cause: Not terminated yet
```

To display MAC-Authentication statistics for port1.0.6 enter the command:

```
awplus# show auth-mac interface port1.0.6 statistics
```

To display the MAC authenticated supplicant on interface port1.0.6, enter the command:

```
awplus# show auth-mac interface port1.0.6 supplicant
```

**Related  
Commands**

[show auth-web diagnostics](#)

[show dot1x sessionstatistics](#)

[show dot1x statistics interface](#)

[show dot1x supplicant interface](#)

# show auth-mac sessionstatistics

**Overview** This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

**Syntax** show auth-mac sessionstatistics [interface <interface-list>]

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface        | Specify an interface to show.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <interface-list> | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• an interface (e.g. v lan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v lan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |

**Mode** Privileged Exec

**Example** To display output displaying MAC-Authentication session statistics for port1.0.2, enter the command:

```
awplus# show auth-mac sessionstatistics interface port1.0.2
```

**Output** Figure 28-4: Example output from the **show auth-mac sessionstatistics** command

```
Authentication
session statistics for interface port1.0.2
 session user name: manager
 session authentication method: Remote server
 session time: 19440 secs
 session terminat cause: Not terminated yet
```

# show auth-mac statistics interface

**Overview** This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

**Syntax** show auth-mac statistics [interface <interface-list>]

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface        | Specify ports to show.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <interface-list> | <p>The interfaces or ports to configure. An interface-list can be:</p> <ul style="list-style-type: none"><li>• an interface (e.g. v l a n 2), a switch port (e.g. p o r t 1 . 0 . 6), a static channel group (e.g. s a 2) or a dynamic (LACP) channel group (e.g. p o 2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v l a n 2 - 8, or p o r t 1 . 0 . 1 - 1 . 0 . 4, or s a 1 - 2, or p o 1 - 2</li><li>• a comma-separated list of the above; e.g. p o r t 1 . 0 . 1, p o r t 1 . 0 . 4 - 1 . 0 . 6. Do not mix interface types in a list</li></ul> <p>The specified interfaces must exist.</p> |

**Mode** Privileged Exec

**Example** To display MAC-Authentication statistics for p o r t 1 . 0 . 2, enter the command:  
awplus# show auth-mac statistics interface port1.0.2

# show auth-mac supplicant

**Overview** This command shows the supplicant (client device) state when MAC-Authentication is configured for the switch. This command shows a summary when the optional **brief** parameter is used.

**Syntax** show auth-mac supplicant [<macadd>] [brief]

| Parameter | Description                                                                                |
|-----------|--------------------------------------------------------------------------------------------|
| <macadd>  | Mac (hardware) address of the Supplicant.<br>Entry format is HHHH.HHHH.HHHH (hexadecimal). |
| brief     | Brief summary of the Supplicant state.                                                     |

**Mode** Privileged Exec

**Example** To display the MAC authenticated supplicant for MAC address 00d0.59ab.7037, enter the command:

```
awplus# show auth-mac supplicant 00d0.59ab.7037
```

```
Web authentication server
 Server status: enabled
 Server address: -
 HTTP Port No: 80
 Security: enabled
 Certification: default
 SSL Port No: 443
 Redirect URL:
 Redirect Delay Time: 30
 HTTP Redirect: disabled
 Session keep: disabled
 PingPolling: disable
 PingInterval: 30
 Timeout: 1
 FailCount: 5
 ReauthFresh: disabled
```



# show auth-mac supplicant interface

**Overview** This command shows the supplicant (client device) state for the MAC authenticated interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port. This command shows a summary when the optional **brief** parameter is used.

**Syntax** show auth-mac supplicant [interface <interface-list>] [brief]

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface        | Specify ports to show.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <interface-list> | <p>The interfaces or ports to configure. An interface-list can be:</p> <ul style="list-style-type: none"><li>• an interface (e.g. vlan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. vlan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</li></ul> <p>The specified interfaces must exist.</p> |
| brief            | Brief summary of the supplicant state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

**Mode** Privileged Exec

**Examples** To display the MAC authenticated supplicant on the interface port1.0.2, enter the command:

```
awplus# show auth-mac supplicant interface port1.0.2
```

# show auth-web

**Overview** This command shows authentication information for Web-based authentication.

**Syntax** show auth-web [all]

| Parameter | Description                                                                                                                                                                           |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| all       | Display all authentication information for each authenticated interface. This can be a static channel (or static aggregator), or a dynamic (or LACP) channel group, or a switch port. |

**Mode** Privileged Exec

**Example** To display all Web-Authentication information, enter the command:

```
awplus# show auth-web all
```

**Output** Figure 28-5: Example output from the **show auth-web** command

```
awplus# show auth-web all
802.1X Port-Based Authentication Enabled
MAC-based Port Authentication Disabled
WEB-based Port Authentication Enabled
 RADIUS server address (auth): 150.87.17.192:1812
 Last radius message id: 4
Authentication Info for interface port1.0.1 portEnabled: true - portControl: Auto
 portStatus: Authorized
 reAuthenticate: disabled
 reAuthPeriod: 3600
 PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in
 KT: keyTxEnabled: false
 critical: disabled
 guestVlan: disabled
 authFailVlan: disabled
 dynamicVlanCreation: disabled
 hostMode: single-host
 dot1x: enabled
 protocolVersion: 1
 authMac: disabled
 authWeb: enabled
 method: PAP
 maxAuthFail: 3
 packetForwarding:
 10.0.0.1 80/tcp
 dns
 dhcp
```

```
twoStepAuthentication:
 configured: enabled
 actual: enabled
supplicantMac: none
Supplicant name: oha
Supplicant address: 000d.6013.5398
authenticationMethod: WEB-based Authentication
Two-Step Authentication:
 firstAuthentication: Pass - Method: dot1x
 secondAuthentication: Pass - Method: web
portStatus: Authorized - currentId: 3
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: 2
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
```

**Related** [show dot1x](#)  
**Commands** [show auth-mac](#)

## show auth-web diagnostics

**Overview** This command shows Web-Authentication diagnostics, optionally for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

**Syntax** show auth-web diagnostics [interface <interface-list>]

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface        | Specify ports to show.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <interface-list> | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• an interface (e.g. v lan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v lan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li><li>• a comma-separated list of the above; e.g. port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |

**Mode** Privileged Exec

**Example** To display authentication diagnostics for port1.0.6, enter the command:

```
awplus# show auth-web diagnostics interface port1.0.6
```

**Output** Figure 28-6: Example output from the **show auth-web diagnostics** command

```
Authentication Diagnostics for interface port1.0.6
 Supplicant address: 00d0.59ab.7037
 authEnterConnecting: 2
 authEaplogoffWhileConnecting: 1
 authEnterAuthenticating: 2
 authSuccessWhileAuthenticating: 1
 authTimeoutWhileAuthenticating: 1
 authFailWhileAuthenticating: 0
 authEapstartWhileAuthenticating: 0
 authEaplogoggWhileAuthenticating: 0
 authReauthsWhileAuthenticated: 0
 authEapstartWhileAuthenticated: 0
 authEaplogoffWhileAuthenticated: 0
 BackendResponses: 2
 BackendAccessChallenges: 1
 BackendOtherrequestToSupplicant: 3
 BackendAuthSuccess: 1
```

**Related  
Commands** [show dot1x interface](#)

# show auth-web interface

**Overview** This command shows the status for Web based authentication on the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interface. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interface. Use the optional **statistics** parameter to show authentication diagnostics for the specified interface. Use the optional **supplicant** (client device) parameter to show the supplicant state for the specified interface.

**Syntax** show auth-web interface <interface-list>  
[diagnostics|sessionstatistics|statistics|supplicant [brief]]

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface-list>  | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"> <li>an interface (e.g. vlan2), a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2)</li> <li>a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. vlan2-8, or port1.0.1-1.0.4, or sa1-2, or po1-2</li> <li>a comma-separated list of the above; e.g. port1.0.1, port1.0.4-1.0.6. Do not mix interface types in a list</li> </ul> The specified interfaces must exist. |
| diagnostics       | Diagnostics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| sessionstatistics | Session statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| statistics        | Statistics.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| supplicant        | Supplicant (client device).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| brief             | Brief summary of supplicant state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Mode** Privileged Exec

**Example** To display the Web based authentication status for port1.0.6, enter the command:

```
awplus# show auth-web interface port1.0.6
```

If web-based authentication is not configured, the output will be

```
% Port-Control not configured on port1.0.6
```

To display the Web based authentication status for port1.0.1, enter the command:

```
awplus# show auth-web interface port1.0.1
```

```
awplus# show auth-web interface port1.0.1
Authentication Info for interface port1.0.1
portEnabled: true - portControl: Auto
portStatus: Authorized
reAuthenticate: disabled
reAuthPeriod: 3600
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in
KT: keyTxEnabled: false
critical: disabled
guestVlan: disabled
authFailVlan: disabled
dynamicVlanCreation: disabled
hostMode: single-host
dot1x: enabled
 protocolVersion: 1
authMac: disabled
authWeb: enabled
 method: PAP
 maxAuthFail: 3
 packetForwarding:
 10.0.0.1 80/tcp
 dns
 dhcp
twoStepAuthentication:
 configured: enabled
 actual: enabled
supplicantMac: none
```

To display Web-Authentication diagnostics for port1.0.6, enter the command:

```
awplus# show auth-web interface port1.0.6 diagnostics
```

```
Authentication Diagnostics for interface port1.0.6

Supplicant address: 00d0.59ab.7037
authEnterConnecting: 2
authEaplogoffWhileConnecting: 1
 authEnterAuthenticating: 2
 authSuccessWhileAuthenticating: 1
 authTimeoutWhileAuthenticating: 1
 authFailWhileAuthenticating: 0
 authEapstartWhileAuthenticating: 0
 authEaplogoggWhileAuthenticating: 0
 authReauthsWhileAuthenticated: 0
 authEapstartWhileAuthenticated: 0
 authEaplogoffWhileAuthenticated: 0
BackendResponses: 2
BackendAccessChallenges: 1
BackendOtherrequestToSupplicant: 3
BackendAuthSuccess: 1
```

To display Web-Authentication session statistics for port1.0.6, enter the command:

```
awplus# show auth-web interface port1.0.6 sessionstatistics
```

```
Authentication
session statistics for interface port1.0.6
 session user name: manager
 session authentication method: Remote server
 session time: 19440 secs
 session terminat cause: Not terminated yet
```

To display Web-Authentication statistics for port1.0.6, enter the command:

```
awplus# show auth-web statistics interface port1.0.6
```

To display the Web-Authenticated supplicant on interface port1.0.6, enter the command:

```
awplus# show auth-web interface port1.0.6 supplicant
```

**Related  
Commands**

[show auth-web diagnostics](#)

[show dot1x sessionstatistics](#)

[show dot1x statistics interface](#)

[show dot1x supplicant interface](#)



# show auth-web sessionstatistics

**Overview** This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

**Syntax** show auth-web sessionstatistics [interface <interface-list>]

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| interface        | Specify ports to show.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| <interface-list> | <p>The interfaces or ports to configure. An interface-list can be:</p> <ul style="list-style-type: none"><li>• an interface (e.g. v l a n 2), a switch port (e.g. p o r t 1 . 0 . 6), a static channel group (e.g. s a 2) or a dynamic (LACP) channel group (e.g. p o 2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v l a n 2 - 8, or p o r t 1 . 0 . 1 - 1 . 0 . 4, or s a 1 - 2, or p o 1 - 2</li><li>• a comma-separated list of the above; e.g. p o r t 1 . 0 . 1, p o r t 1 . 0 . 4 - 1 . 0 . 6. Do not mix interface types in a list</li></ul> <p>The specified interfaces must exist.</p> |

**Mode** Privileged Exec

**Example** To display authentication statistics for p o r t 1 . 0 . 6, enter the command:  
awplus# show auth-web sessionstatistics interface port1.0.6

**Output** Figure 28-7: Example output from the **show auth-web sessionstatistics** command

```
Authentication
session statistics for interface port1.0.6
 session user name: manager
 session authentication method: Remote server
 session time: 19440 secs
 session terminat cause: Not terminated yet
```

# show auth-web statistics interface

**Overview** This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

**Syntax** show auth-web statistics interface *<interface-list>*

| Parameter                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;interface-list&gt;</i> | <p>The interfaces or ports to configure. An interface-list can be:</p> <ul style="list-style-type: none"><li>• an interface (e.g. <code>vlan2</code>), a switch port (e.g. <code>port1.0.6</code>), a static channel group (e.g. <code>sa2</code>) or a dynamic (LACP) channel group (e.g. <code>po2</code>)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. <code>vlan2-8</code>, or <code>port1.0.1-1.0.4</code>, or <code>sa1-2</code>, or <code>po1-2</code></li><li>• a comma-separated list of the above; e.g. <code>port1.0.1, port1.0.4-1.0.6</code>. Do not mix interface types in a list</li></ul> <p>The specified interfaces must exist.</p> |

**Mode** Privileged Exec

**Example** To display Web-Authentication statistics for `port1.0.4`, enter the command:

```
awplus# show dot1x statistics interface port1.0.4
```

**Related Commands** [show dot1x interface](#)

# show auth-web supplicant

**Overview** This command shows the supplicant (client device) state when Web-Authentication is configured for the switch. This command shows a summary when the optional **brief** parameter is used.

**Syntax** show auth-web supplicant [<macadd>] [brief]

| Parameter | Description                                                                                |
|-----------|--------------------------------------------------------------------------------------------|
| <macadd>  | Mac (hardware) address of the supplicant.<br>Entry format is HHHH.HHHH.HHHH (hexadecimal). |
| brief     | Brief summary of the supplicant state.                                                     |

**Mode** Privileged Exec

**Examples** To display Web authenticated supplicant information on the switch, enter the command:

```
awplus# show auth-web supplicant
```

# show auth-web supplicant interface

**Overview** This command shows the supplicant (client device) state for the Web authenticated interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port. This command shows a summary when the optional **brief** parameter is used.

**Syntax** show auth-web supplicant interface *<interface-list>* [brief]

| Parameter                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;interface-list&gt;</i> | The interfaces or ports to configure. An interface-list can be: <ul style="list-style-type: none"><li>• an interface (e.g. v l a n 2), a switch port (e.g. p o r t 1 . 0 . 6), a static channel group (e.g. s a 2) or a dynamic (LACP) channel group (e.g. p o 2)</li><li>• a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. v l a n 2 - 8, or p o r t 1 . 0 . 1 - 1 . 0 . 4, or s a 1 - 2, or p o 1 - 2</li><li>• a comma-separated list of the above; e.g. p o r t 1 . 0 . 1, p o r t 1 . 0 . 4 - 1 . 0 . 6. Do not mix interface types in a list</li></ul> The specified interfaces must exist. |
| brief                         | Brief summary of the supplicant state.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |

**Mode** Privileged Exec

**Examples** To display the Web authenticated supplicant on the interface p o r t 1 . 0 . 3, enter the command:

```
awplus# show auth-web supplicant interface port1.0.3
```

To display brief summary output for the Web authenticated supplicant, enter the command:

```
awplus# show auth-web supplicant brief
```

# show auth-web-server

**Overview** This command shows the Web-Authentication server configuration and status on the switch.

**Syntax** show auth-web-server

**Mode** Privileged Exec

**Example** To display Web-Authentication server configuration and status, enter the command:

```
awplus# show auth-web-server
```

**Output** Figure 28-8: Example output from the **show auth-web-server** command

```
Web authentication server
 Server status: enabled
 Server mode: none
 Server address: 192.168.1.1/24
 DHCP server enabled
 DHCP lease time: 20
 DHCP WPAD Option URL: http://192.168.1.1/proxy.pac
 HTTP Port No: 80
 Security: disabled
 Certification: default
 SSL Port No: 443
 Redirect URL: --
 Redirect Delay Time: 5
 HTTP Redirect: enabled
 Session keep: disabled
 PingPolling: disabled
 PingInterval: 30
 Timeout: 1
 FailCount: 5
 ReauthTimerReFresh: disabled
```

**Related Commands**

- [auth-web-server gateway \(deleted\)](#)
- [auth-web-server http-redirect \(deleted\)](#)
- [auth-web-server ipaddress](#)
- [auth-web-server port](#)
- [auth-web-server redirect-delay-time](#)
- [auth-web-server redirect-url](#)
- [auth-web-server session-keep](#)
- [auth-web-server ssl](#)
- [auth-web-server sslport \(deleted\)](#)

# show auth-web-server page

**Overview** This command displays the web-authentication page configuration and status.

**Syntax** show auth-web-server page

**Mode** Privileged Exec

**Examples** To show the web-authentication page information, use the command:

```
awplus# show auth-web-server page
```

Table 28-1: Example output from the **show auth-web-server page** command on the console.

```
awplus#show auth-web-server page
Web authentication page
Logo: auto
Title: default
Sub-Title: Web Authentication
Welcome message: Your welcome message
Success message: Your success message
```

**Related Commands**

- [auth-web forward](#)
- [auth-web-server page logo](#)
- [auth-web-server page sub-title](#)
- [auth-web-server page success-message](#)
- [auth-web-server page title](#)
- [auth-web-server page welcome-message](#)

# show proxy-autoconfig-file

**Overview** This command displays the contents of the proxy auto configuration (PAC) file.

**Syntax** show proxy-autoconfig-file

**Mode** Privileged Exec

**Example** To display the contents of the proxy auto configuration (PAC) file, enter the command:

```
awplus# show auth proxy-autoconfig-file
```

**Output** Figure 28-9: Example output from the **show proxy-autoconfig-file**

```
function FindProxyForURL(url,host)
{
 if (isPlainHostName(host) ||
 isInNet(host, "192.168.1.0", "255.255.255.0")) {
 return "DIRECT";
 }
 else {
 return "PROXY 192.168.110.1:8080";
 }
}
```

**Related Commands** [copy proxy-autoconfig-file](#)  
[erase proxy-autoconfig-file](#)

# 29

# AAA Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for AAA commands for Authentication, Authorization and Accounting. For more information, see the [AAA Feature Overview and Configuration Guide](#).

- Command List**
- [“aaa accounting auth-mac default”](#) on page 946
  - [“aaa accounting auth-web default”](#) on page 948
  - [“aaa accounting commands”](#) on page 950
  - [“aaa accounting dot1x”](#) on page 952
  - [“aaa accounting login”](#) on page 954
  - [“aaa accounting update”](#) on page 957
  - [“aaa authentication auth-mac”](#) on page 959
  - [“aaa authentication auth-web”](#) on page 960
  - [“aaa authentication dot1x”](#) on page 961
  - [“aaa authentication enable default group tacacs+”](#) on page 962
  - [“aaa authentication enable default local”](#) on page 964
  - [“aaa authentication login”](#) on page 965
  - [“aaa group server”](#) on page 967
  - [“aaa local authentication attempts logout-time”](#) on page 969
  - [“aaa local authentication attempts max-fail”](#) on page 970
  - [“accounting login”](#) on page 971
  - [“clear aaa local user logout”](#) on page 972
  - [“debug aaa”](#) on page 973
  - [“login authentication”](#) on page 974



- [“show aaa local user locked”](#) on page 975
- [“show debugging aaa”](#) on page 976
- [“undebug aaa”](#) on page 977

## aaa accounting auth-mac default

**Overview** This command configures a default accounting method list for MAC-based Authentication. The default accounting method list specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to interfaces with MAC-based Authentication enabled.

Use the **no** variant of this command to disable AAA accounting for MAC-based Authentication globally.

**Syntax** `aaa accounting auth-mac default {start-stop|stop-only|none}  
group {<group-name>|radius}  
no aaa accounting auth-mac default`

| Parameter    | Description                        |
|--------------|------------------------------------|
| start-stop   | Start and stop records to be sent. |
| stop-only    | Stop records to be sent.           |
| none         | No accounting record to be sent.   |
| <group-name> | Server group name.                 |
| radius       | Use all RADIUS servers             |

**Default** RADIUS accounting for MAC-based Authentication is disabled by default

**Mode** Global Configuration

**Usage** 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

The accounting event to send to the RADIUS 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.

Use the no variant of this command to disable AAA accounting for MAC-based Authentication globally.

**Examples** To enable RADIUS accounting for MAC-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-mac default start-stop
group radius
```

To disable RADIUS accounting for MAC-based Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-mac default
```

**Related  
Commands** [aaa authentication auth-mac](#)

# aaa accounting auth-web default

**Overview** This command configures a default accounting method list for Web-based Port Authentication. The default accounting method list specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to interfaces with Web-based Authentication enabled.

Use the **no** variant of this command to disable AAA accounting for Web-based Port Authentication globally.

**Syntax** `aaa accounting auth-web default {start-stop|stop-only|none}  
group {<group-name>|radius}  
no aaa accounting auth-web default`

| Parameter    | Description                        |
|--------------|------------------------------------|
| start-stop   | Start and stop records to be sent. |
| stop-only    | Stop records to be sent.           |
| none         | No accounting record to be sent.   |
| <group-name> | Server group name.                 |
| radius       | Use all RADIUS servers.            |

**Default** RADIUS accounting for Web-based Port Authentication is disabled by default.

**Mode** Global Configuration

**Usage** 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

Configure the accounting event to be sent to the RADIUS server 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 enable RADIUS accounting for Web-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-web default start-stop
group radius
```

To disable RADIUS accounting for Web-based Authentication, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no aaa accounting auth-web default
```

**Related  
Commands**    [aaa authentication auth-web](#)

# aaa accounting commands

**Overview** Use this command to configure and enable TACACS+ command accounting. When command accounting is enabled, information about a command entered at a specified privilege level on a device is sent to a TACACS+ server. To account for all commands entered on a device you need to configure command accounting for each discrete privilege level. A command accounting record includes the command as entered for the specified privilege level, the date and time each command execution finished, and the username of the user who executed the command.

This command creates a default method list that is applied to every console and vty line. The **stop-only** parameter indicates that an accounting message is sent to the TACACS+ server when a command has stopped executing.

Note that up to four TACACS+ servers can be configured for accounting. The servers are checked for reachability in the order they are configured and only the first reachable server is used. If no server is found the accounting message is dropped.

Use the **no** variant of this command to disable command accounting.

**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, in the range 1 to 15. |

**Default** TACACS+ command accounting is disabled by default.

**Mode** Global Configuration

**Usage** When command accounting is enabled, the command as entered is included in the accounting packets sent to the TACACS+ accounting server.

You cannot enable command accounting if a trigger is configured. An error message is displayed if you attempt to enable command accounting and a trigger is configured.

The [show tech-support](#) command runs a number of commands and each command is accounted separately.

When the **copy <filename> running-config** command is executed all the commands of a configuration file copied into the running-config are accounted separately.

**Examples** To configure command accounting for privilege level 15 commands, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa accounting commands 15 default stop-only
group tacacs+
```

To disable command accounting for privilege level 15 commands, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no aaa accounting commands 15 default
```

**Related  
Commands**

- [aaa authentication login](#)
- [aaa accounting login](#)
- [accounting login](#)
- [tacacs-server host](#)

# aaa accounting dot1x

**Overview** This command configures the default accounting method list for IEEE 802.1X-based Authentication. The default accounting method list specifies what type of accounting messages are sent and specifies which RADIUS Servers the accounting messages are sent to. The default accounting method list is automatically applied to interfaces with IEEE 802.1X-based Authentication enabled.

Use the **no** variant of this command to disable AAA accounting for 802.1X-based Port Authentication globally.

**Syntax** `aaa accounting dot1x default {start-stop|stop-only|none} group {<group-name>|radius}`  
`no aaa accounting dot1x default`

| Parameter    | Description                        |
|--------------|------------------------------------|
| start-stop   | Start and stop records to be sent. |
| stop-only    | Stop records to be sent.           |
| none         | No accounting record to be sent.   |
| <group-name> | Server group name.                 |
| radius       | Use all RADIUS servers.            |

**Default** RADIUS accounting for 802.1X-based Port Authentication is disabled by default (there is no default server set by default).

**Mode** Global Configuration

**Usage** 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.

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.



**Examples** To enable RADIUS accounting for 802.1X-based Authentication, and use all available RADIUS Servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting dot1x default start-stop group
radius
```

To disable RADIUS accounting for 802.1X-based Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting dot1x default
```

**Related  
Commands**

- [aaa accounting update](#)
- [aaa authentication dot1x](#)
- [aaa group server](#)
- [dot1x port-control](#)
- [radius-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** 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 `<list-name>` for any method list that you define can then be used as the `<list-name>` parameter in the `accounting login` command available from Line Configuration mode.

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](#)
- [aaa accounting update](#)
- [accounting login](#)
- [radius-server host](#)
- [tacacs-server host](#)

# 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** Periodic accounting update is disabled by default.

**Mode** Global Configuration

**Usage** Use this command to enable the device to send periodic AAA login accounting reports to the accounting server. When periodic accounting report is enabled, interim accounting records are sent according to 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 reenabled, 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 update wherever accounting has been configured, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no aaa accounting update
```

**Related  
Commands**

[aaa accounting auth-mac default](#)

[aaa accounting auth-web default](#)

[aaa accounting dot1x](#)

[aaa accounting login](#)

# aaa authentication auth-mac

**Overview** This command enables MAC-based Port Authentication globally and allows you to specify an authentication method list. It is automatically applied to every interface running MAC-based Port Authentication.

Use the **no** variant of this command to globally disable MAC-based Port Authentication.

**Syntax** `aaa authentication auth-mac default group {<group-name>|radius}`  
`no aaa authentication auth-mac default`

| Parameter                       | Description             |
|---------------------------------|-------------------------|
| <code>&lt;group-name&gt;</code> | Server group name.      |
| <code>radius</code>             | Use all RADIUS servers. |

**Default** MAC-based Port Authentication is disabled by default.

**Mode** Global Configuration

**Usage** 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

All configured RADIUS Servers are automatically members of the server group **radius**. If a server is added to a named group **<group-name>**, it also remains a member of the group **radius**.

**Examples** To enable MAC-based Port Authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-mac default group
radius
```

To disable MAC-based Port Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-mac default
```

**Related Commands** [aaa accounting auth-mac default](#)  
[auth-mac enable](#)

# aaa authentication auth-web

**Overview** This command enables Web-based Port Authentication globally and allows you to enable an authentication method list (in this case, a list of RADIUS Servers). It is automatically applied to every interface running Web-based Port Authentication.

Use the **no** variant of this command to globally disable Web-based Port Authentication.

**Syntax** `aaa authentication auth-web default group {<group-name>|radius}`  
`no aaa authentication auth-web default`

| Parameter                       | Description             |
|---------------------------------|-------------------------|
| <code>&lt;group-name&gt;</code> | Server group name.      |
| <code>radius</code>             | Use all RADIUS servers. |

**Default** Web-based Port Authentication is disabled by default.

**Mode** Global Configuration

**Usage** 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

Note that you need to configure an IPv4 address for the VLAN interface on which We Authentication is running.

**Examples** To enable Web-based Port Authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-web default group
radius
```

To disable Web-based Port Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-web default
```

**Related Commands** [aaa accounting auth-web default](#)  
[auth-mac enable](#)



# aaa authentication dot1x

**Overview** This command enables 802.1X-based Port Authentication globally and allows you to enable an authentication method list. It is automatically applied to every interface running 802.1X-based Port Authentication.

Use the **no** variant of this command to globally disable 802.1X-based Port Authentication.

**Syntax** `aaa authentication dot1x default group {<group-name>|radius}`  
`no aaa authentication dot1x default`

| Parameter    | Description             |
|--------------|-------------------------|
| radius       | Use all RADIUS servers. |
| <group-name> | Server group name.      |

**Default** 802.1X-based Port Authentication is disabled by default.

**Mode** Global Configuration

**Usage** Use this command to specify the default method list to use for authentication on all switch ports with 802.1X enabled. Use the **no** variant of this command to reset the authentication method list for 802.1X to its default (i.e. to use the group **radius**, containing all RADIUS servers configured by the **radius-server host** command).

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

**Examples** To enable 802.1X-based Port Authentication globally with all RADIUS servers, and use all available RADIUS servers, use the command:

```
awplus# configure terminal
awplus(config)# aaa authentication dot1x default group radius
```

To disable 802.1X-based Port Authentication, use the command:

```
awplus# configure terminal
awplus(config)# no aaa authentication dot1x default
```

**Related Commands** [aaa accounting dot1x](#)  
[aaa group server](#)  
[dot1x port-control](#)  
[radius-server host](#)

# aaa authentication enable default group tacacs+

**Overview** This command enables AAA authentication to determine the privilege level a user can access for passwords authenticated against the 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** 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](#)
- [tacacs-server host](#)

# aaa authentication enable default local

**Overview** This command enables AAA authentication to determine the privilege level a user can access for passwords authenticated locally.

**Syntax** `aaa authentication enable default local`

**Default** Local privilege level authentication is enabled by default.

**Mode** Global Configuration

**Usage** 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 command, use the following commands:

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

To disable privilege level authentication, use the following commands:

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

**Related Commands**

- [aaa authentication enable default group tacacs+](#)
- [aaa authentication login](#)
- [enable \(Privileged Exec mode\)](#)
- [enable password](#)
- [enable secret](#)
- [tacacs-server host](#)

# aaa authentication login

**Overview** Use this command to create an ordered list of methods to use to authenticate user login, or to replace an existing method list with 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 an authentication method list for user login. 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|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.                  |
| 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** 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. Reset to the default method list using the **no aaa authentication login default** command.

**Mode** Global Configuration

**Usage** 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 not 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 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+](#)  
[login authentication](#)

## aaa group server

**Overview** This command configures a RADIUS server group. A server group can be used to specify a subset of RADIUS servers in **aaa** commands. The group name **radius** is predefined, which includes all RADIUS servers configured by the **radius-server host** command.

RADIUS servers are added to a server group using the **server** command. Each RADIUS server should be configured using the **radius-server host** command.

Use the **no** variant of this command to remove an existing RADIUS server group.

**Syntax** `aaa group server radius <group-name>`  
`no aaa group server radius <group-name>`

| Parameter                       | Description        |
|---------------------------------|--------------------|
| <code>&lt;group-name&gt;</code> | Server group name. |

**Mode** Global Configuration

**Usage** Use this command to create an AAA group of RADIUS servers, and to enter Server Group Configuration mode, in which you can add servers to the group. Use a server group to specify a subset of RADIUS servers in AAA commands. Each RADIUS server must be configured by the **radius-server host** command. To add RADIUS servers to a server group, use the **server** command.

**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
```

**Related  
Commands**

aaa accounting auth-mac default  
aaa accounting auth-web default  
aaa accounting dot1x  
aaa accounting login  
aaa authentication auth-mac  
aaa authentication auth-web  
aaa authentication dot1x  
aaa authentication login  
radius-server host  
server (Server Group)



# 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** 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

**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](#)  
[clear aaa local user lockout](#)

# 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 (Authentication, Authorization, Accounting) 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 beforehand.

**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
```

**Related Commands** [aaa accounting commands](#)  
[aaa accounting login](#)

# 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 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](#)

# show aaa local user locked

**Overview** This command displays the current number of failed attempts, last failure time and location against each user account attempting to log into the device.

Note that once the lockout count has been manually cleared by another privileged account using the [clear aaa local user lockout](#) command or a locked account successfully logs into the system after waiting for the lockout time, this command will display nothing for that particular account.

**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 29-1: Example output from the **show aaa local user locked** command

|                                    |          |                |          |               |
|------------------------------------|----------|----------------|----------|---------------|
| awplus# show aaa local user locked |          |                |          |               |
| Login                              | Failures | Latest failure |          | From          |
| bob                                | 3        | 05/23/14       | 16:21:37 | ttyS0         |
| manager                            | 5        | 05/23/14       | 16:31:44 | 192.168.1.200 |

**Related Commands**

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

# show debugging aaa

**Overview** This command displays the current debugging status 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 29-2: Example output from the **show debug aaa** command

```
AAA debugging status:
Authentication debugging is on
Accounting debugging is off
```



# undebbug aaa

**Overview** This command applies the functionality of the **no debug aaa** command.

# 30

# RADIUS Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure the device to use RADIUS servers.

- Command List**
- “[deadtime \(RADIUS server group\)](#)” on page 979
  - “[debug radius](#)” on page 980
  - “[ip radius source-interface](#)” on page 981
  - “[radius-server deadtime](#)” on page 982
  - “[radius-server host](#)” on page 983
  - “[radius-server key](#)” on page 986
  - “[radius-server retransmit](#)” on page 987
  - “[radius-server timeout](#)” on page 989
  - “[server \(Server Group\)](#)” on page 991
  - “[show debugging radius](#)” on page 993
  - “[show radius](#)” on page 994
  - “[show radius statistics](#)” on page 996
  - “[undebug radius](#)” on page 997

# 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** 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 command:

```
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 command:

```
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 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                                      |
|--------------|--------------------------------------------------|
| <interface>  | Interface name.                                  |
| <ip-address> | 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](#)  
[show radius statistics](#)

# 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](#)  
[show radius statistics](#)

# 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<br>(Accounting port number is set to 1813 by default)<br>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<br>(Authentication port number is set to 1812 by default)<br>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)<br>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.<br>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)<br>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.<br>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<br>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. 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 c</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 **allied** 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 allied
```

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](#)  
[show radius statistics](#)

# 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>  
no radius-server key

| Parameter | Description                                          |
|-----------|------------------------------------------------------|
| <key>     | 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 c** ommand, 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](#)  
[show radius statistics](#)

# 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
- show radius statistics

# 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                                                                                                                                                                                                                                                               |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <seconds> | 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](#)  
[show radius statistics](#)

# server (Server Group)

**Overview** This command adds a RADIUS server to a server group in Server-Group Configuration mode. The RADIUS server should be configured by the [radius-server host](#) command.

The server is appended to the server list of the group and the order of configuration determines the precedence of servers. If the server exists in the server group already, it will be removed before added as a new server.

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** Server Group Configuration

**Usage** 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 auth-mac default](#)
- [aaa accounting auth-web default](#)
- [aaa accounting dot1x](#)
- [aaa accounting login](#)
- [aaa authentication auth-mac](#)
- [aaa authentication auth-web](#)
- [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 30-1: 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 30-2: 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 30-3: 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
show radius local-server group

```

| 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.                                                                                                                           |
| 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 statistics

**Overview** This command shows the RADIUS client statistics for the device.

**Syntax** show radius statistics

**Mode** User Exec and Privileged Exec

**Example** See the sample output below showing RADIUS client statistics and RADIUS configuration:

```
awplus# show radius statistics
```

**Output** Figure 30-4: Example output from the **show radius statistics** command:

```
RADIUS statistics for Server: 150.87.18.89
Access-Request Tx : 5 - Retransmit : 0
Access-Accept Rx : 1 - Access-Reject Rx : 2
Access-Challenge Rx : 2
Unknown Type : 0 - Bad Authenticator : 0
Malformed Access-Resp : 0 - Wrong Identifier : 0
Bad Attribute : 0 - Packet Dropped : 0
TimeOut : 0 - Dead count : 0
Pending Request : 0
```

# undebbug radius

**Overview** This command applies the functionality of the **no debug radius** command.

# 31

# 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**
- [“show tacacs+”](#) on page 999
  - [“tacacs-server host”](#) on page 1000
  - [“tacacs-server key”](#) on page 1002
  - [“tacacs-server timeout”](#) on page 1003

# 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 31-1: Example output from the **show tacacs+** command

|                              |                  |
|------------------------------|------------------|
| TACACS+ Global Configuration |                  |
| Timeout                      | : 5 sec          |
| Server Host/<br>IP Address   | Server<br>Status |
| -----                        |                  |
| 192.168.1.10                 | Alive            |
| 192.168.1.11                 | Unknown          |

Table 31-1: Parameters in the output of the **show tacacs+** command

| Output Parameter       | Meaning                                                                            |
|------------------------|------------------------------------------------------------------------------------|
| 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.                                    |

# 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+](#)

# 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** 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+](#)

# 32

# 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 1006
  - “[clear ssh](#)” on page 1007
  - “[crypto key destroy hostkey](#)” on page 1008
  - “[crypto key destroy userkey](#)” on page 1009
  - “[crypto key generate hostkey](#)” on page 1010
  - “[crypto key generate userkey](#)” on page 1011
  - “[crypto key pubkey-chain knownhosts](#)” on page 1012
  - “[crypto key pubkey-chain userkey](#)” on page 1014
  - “[debug ssh client](#)” on page 1016
  - “[debug ssh server](#)” on page 1017
  - “[service ssh](#)” on page 1018
  - “[show banner login](#)” on page 1020
  - “[show crypto key hostkey](#)” on page 1021
  - “[show crypto key pubkey-chain knownhosts](#)” on page 1022
  - “[show crypto key pubkey-chain userkey](#)” on page 1023
  - “[show crypto key userkey](#)” on page 1024
  - “[show running-config ssh](#)” on page 1025
  - “[show ssh](#)” on page 1027
  - “[show ssh client](#)” on page 1029

- ["show ssh server"](#) on page 1030
- ["show ssh server allow-users"](#) on page 1032
- ["show ssh server deny-users"](#) on page 1033
- ["ssh"](#) on page 1034
- ["ssh client"](#) on page 1036
- ["ssh server"](#) on page 1038
- ["ssh server allow-users"](#) on page 1040
- ["ssh server authentication"](#) on page 1042
- ["ssh server deny-users"](#) on page 1044
- ["ssh server resolve-host"](#) on page 1046
- ["ssh server scp"](#) on page 1047
- ["ssh server sftp"](#) on page 1048
- ["undebbug ssh client"](#) on page 1049
- ["undebbug ssh server"](#) on page 1050

# 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. Note that for an SSH server to operate it needs at least one set of hostkeys configured before an SSH server is started.

**Syntax** `crypto key destroy hostkey {dsa|rsa|rsa1}`

| Parameters | Description                                                                                |
|------------|--------------------------------------------------------------------------------------------|
| dsa        | Deletes the existing DSA public and private keys.                                          |
| rsa        | Deletes the existing RSA public and private keys configured for SSH version 2 connections. |
| rsa1       | Deletes the existing RSA public and private keys configured for SSH version 1 connections. |

**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](#)



# 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|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.                                                                                                                                                      |
| rsa        | Deletes the existing RSA userkey configured for SSH version 2 connections.                                                                                                             |
| rsa1       | Deletes the existing RSA userkey for SSH version 1 connections.                                                                                                                        |

**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](#)
- [show ssh](#)
- [show crypto key hostkey](#)

# crypto key generate hostkey

**Overview** This command generates public and private keys for the SSH server using either an RSA or DSA cryptography algorithm. You must define a host key before enabling the SSH server. Start SSH server using the **service ssh** command. 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 {dsa|rsa|rsa1} [<768-32768>]`

| Parameters  | Description                                                                          |
|-------------|--------------------------------------------------------------------------------------|
| dsa         | Creates a DSA hostkey. Both SSH version 1 and 2 connections can use the DSA hostkey. |
| rsa         | Creates an RSA hostkey for SSH version 2 connections.                                |
| rsa1        | Creates an RSA hostkey for SSH version 1 connections.                                |
| <768-32768> | The length in bits of the generated key. The default is 1024 bits.                   |

**Default** 1024 bits is the default key length. The DSA algorithm supports 1024 bits.

**Mode** Global Configuration

**Examples** To generate an RSA host key for SSH version 2 connections that is 2048 bits in length, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 2048
```

To generate a DSA host key, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate dsa
```

**Related Commands**

- [crypto key destroy hostkey](#)
- [service ssh](#)
- [show crypto key hostkey](#)

# crypto key generate userkey

**Overview** This command generates public and private keys for an SSH user using either an RSA or DSA 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> {dsa|rsa|rsa1} [<768-32768>]`

| 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. |
| dsa         | Creates a DSA userkey. Both SSH version 1 and 2 connections can use a key created with this command.                                                                                     |
| rsa         | Creates an RSA userkey for SSH version 2 connections.                                                                                                                                    |
| rsa1        | Creates an RSA userkey for SSH version 1 connections.                                                                                                                                    |
| <768-32768> | The length in bits of the generated key. The DSA algorithm supports only 1024 bits. Default: 1024.                                                                                       |

**Mode** Global Configuration

**Examples** To generate a 2048-bits 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 2048
```

To generate a DSA user key for the user lapo, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo dsa
```

**Related Commands** [crypto key pubkey-chain userkey](#)  
[show crypto key userkey](#)

# 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>  
[rsa|dsa|rsa1]  
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. |
| rsa        | Specify the RSA public key of the server to be added to the known host database.                                                                        |
| dsa        | Specify the DSA public key of the server to be added to the known host database.                                                                        |
| rsa1       | Specify the SSHv1 public key of the server to be added to the know 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** 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`

# 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** 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
rsaAAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fc0w1TStpb9J20bWluh
```

```
nUC768EoWhyPW6FZ2t536005M29EpKBmGqlkQaz5V0mU9IQe66+5YyD4Ux0KSD
tTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/pqGDijj4SvfZZfe
ITzvvyZW4/I4pbN8=
```

```
awplus# configure terminal
```

```
awplus(config)# crypto key pubkey-chain userkey joeType CNTL/D
to
```

```
finish:AAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fc0w1TStpb9J20b
WluhnUC768EoWhyPW6FZ2t536005M29EpKBmGqlkQaz5V0mU9IQe66+5YyD4Ux
OKSDtTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/pqGDijj4Svf
ZZfeITzvvyZW4/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](#)



# 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** This command enables the Secure Shell server on the device. Once enabled, connections coming from SSH clients are accepted.

SSH server needs a host key before it starts. If an SSHv2 host key does not exist, then this command fails. If SSHv1 is enabled but a host key for SSHv1 does not exist, then SSH service is unavailable for version 1.

The **no** variant of this command disables 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

# 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 SSH host keys generated by RSA and DSA algorithm. A host key pair (public and private keys) is needed to enable SSH server. The private key remains on the device secretly. The public key is copied to SSH clients to identify the server

**Syntax** show crypto key hostkey [dsa|rsa|rsa1]

| Parameter | Description                                                          |
|-----------|----------------------------------------------------------------------|
| dsa       | Displays the DSA 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. |

**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 32-1: Example output from the **show crypto key hostkey** command

| Type | Bits | Fingerprint                                     |
|------|------|-------------------------------------------------|
| rsa  | 2058 | 4e:7d:1d:00:75:79:c5:cb:c8:58:2e:f9:29:9c:1f:48 |
| dsa  | 1024 | fa:72:3d:78:35:14:cb:9a:1d:ca:1c:83:2c:7d:08:43 |
| rsa1 | 1024 | e2:1c:c8:8b:d8:6e:19:c8:f4:ec:00:a2:71:4e:85:8b |

Table 32-1: 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 32-2: 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 32-2: 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](#)

# 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 32-3: 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 32-3: 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 32-4: 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 32-4: 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 32-5: 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 32-5: 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 32-5: 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 32-6: 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  | 550dev_.awd |  |
| 463                    | ssh  | client | 5ffe:33fe:5632:ffbb:bc35:ddee:0101:ac51 | manager  | user-auth |             |  |

Table 32-6: 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 32-6: 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 32-7: 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 32-7: 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 "1", "2" or "2,1".                                                                                                               |
| 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](#)

## 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 32-8: Example output from the **show ssh server** command

```
Secure Shell Server Configuration

SSH Server : Enabled
Port : 22
Version : 2
Services : scp, sftp
User Authentication : publickey, password
Idle Timeout : 60 seconds
Maximum Startups : 10
Debug : NONE
```

Table 32-8: 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 "1", "2" or "2,1".                                                                                                                                        |
| Services       | List of the available Secure Shell service; one or more of SHELL, SCP or SFTP.                                                                                                       |
| 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. |

Table 32-8: Parameters in the output of the **show ssh server** command (cont.)

| Parameter        | Description                                                                                      |
|------------------|--------------------------------------------------------------------------------------------------|
| Maximum Startups | The maximum number of concurrent connections that are waiting authentication. The default is 10. |
| Debug            | Whether debugging is active on the server.                                                       |

**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 32-9: Example output from the **show ssh server allow-users** command

| Username | Remote Hostname (pattern) |
|----------|---------------------------|
| -----    | -----                     |
| awplus   | 192.168.*                 |
| john     |                           |
| manager  | *.alliedtelesis.com       |

Table 32-9: 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 32-10: Example output from the **show ssh server deny-users** command

| Username | Remote Hostname (pattern) |
|----------|---------------------------|
| john     | *.b-company.com           |
| manager  | 192.168.2.*               |

Table 32-10: 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** This command initiates a Secure Shell connection to a remote SSH server.

If the server requests a password for the user login, the user needs to type in the correct password on "Password:" prompt.

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:** Note that any hostname specified with ssh cannot begin with a hyphen (-) character.

**Syntax** ssh [ip|ipv6][[user <username>]][port <1-65535>][version {1|2}]] <hostname> [<line>]

| 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. Other- wise, 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. If version is specified, the SSH client supports only the specified SSH version. By default, SSH client uses SSHv2 first. If the server does not support SSHv2, it will try SSHv1. The default version can be configured by "ssh client" command.<br><br>1 Use SSH version 1.<br>2 Use SSH version 2. |
| <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 corresponding to the ip or ipv6 optional keywords used. Note that any hostname specified with ssh cannot begin with a hyphen (-) character.                          |
|            | <line> 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 TCP port 2000, use the command:

```
awplus# ssh port 2000 192.0.2.5
```

To login to the remote SSH server with example\_host using 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](#)

# 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 {1|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. The SSH client supports both version 2 and version 1<br>Default: version 2<br>Note: SSH version 2 is the default SSH version. SSH client supports SSH version 1 if SSH version 2 is not configured using a ssh version command.                                                                            |
|                 | 1 SSH clients on the device supports SSH version 1 only.                                                                                                                                                                                                                                                                                                        |
|                 | 2 SSH clients on the device supports SSH version 2 only                                                                                                                                                                                                                                                                                                         |
| 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](#)

## ssh server

**Overview** This command modifies the configuration of the SSH server. Changing these parameters affects new SSH sessions connecting to the device.

The **no** variant of this command restores 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 {[v1v2|v2only]} [<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                                                                                                                                                                                                                                                                                                                    |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| v1v2            | Supports both SSHv2 and SSHv1 client connections.<br>Default: v1v2                                                                                                                                                                                                                                                             |
| v2only          | Supports SSHv2 client connections only.                                                                                                                                                                                                                                                                                        |
| <1-65535>       | The TCP port number that the server listens to for incoming SSH sessions.<br>Default: 22                                                                                                                                                                                                                                       |
| session-timeout | There is a 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). |
| <0-3600>        | Timeout in seconds.                                                                                                                                                                                                                                                                                                            |
| login-timeout   | The maximum time period the server waits before disconnecting an unauthenticated client.<br>Default: 60                                                                                                                                                                                                                        |
| <1-600>         | Timeout in 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                           |
| <1-128>         | Number of sessions.                                                                                                                                                                                                                                                                                                            |

**Mode** Global Configuration

**Examples** To configure the session timer of SSH server to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 600
```

To configure the login timeout of 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 authentication from SSH server to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-startups
```

To set max-startups parameters of SSH server to the default configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server max-startups
```

To support the Secure Shell server with TCP port 2200, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server 2200
```

To force the Secure Shell server to support SSHv2 only, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server v2only
```

To support both SSHv2 and SSHv1, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server v1v2
```

**Related  
Commands** [show ssh server](#)  
[ssh client](#)

# 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 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** Your device has a DNS Client that is enabled automatically when you add a DNS server to your device.

For information about configuring DNS, see the [Internet Protocol Feature Overview and Configuration Guide](#).

**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 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](#)



# undebug ssh client

**Overview** This command applies the functionality of the **no debug ssh client** command.

# undebbug ssh server

**Overview** This command applies the functionality of the **no debug ssh server** command.

# 33

# DHCP Snooping Commands

## Introduction

**Overview** This chapter gives detailed information about the commands used to configure DHCP snooping. For detailed descriptions of related ACL commands, see [IPv4 Hardware Access Control List \(ACL\) Commands](#). For more information about DHCP snooping, see the [DHCP Snooping Feature Overview and Configuration Guide](#).

DHCP snooping can operate on static link aggregators (e.g. sa2) and dynamic link aggregators (e.g. po2), as well as on switch ports (e.g. port1.0.2).

- Command List**
- [“arp security”](#) on page 1053
  - [“arp security violation”](#) on page 1054
  - [“clear arp security statistics”](#) on page 1056
  - [“clear ip dhcp snooping binding”](#) on page 1057
  - [“clear ip dhcp snooping statistics”](#) on page 1058
  - [“debug arp security”](#) on page 1059
  - [“debug ip dhcp snooping”](#) on page 1060
  - [“ip dhcp snooping”](#) on page 1061
  - [“ip dhcp snooping agent-option”](#) on page 1062
  - [“ip dhcp snooping agent-option allow-untrusted”](#) on page 1063
  - [“ip dhcp snooping agent-option circuit-id vlantriplet”](#) on page 1064
  - [“ip dhcp snooping agent-option remote-id”](#) on page 1065
  - [“ip dhcp snooping binding”](#) on page 1066
  - [“ip dhcp snooping database”](#) on page 1067
  - [“ip dhcp snooping delete-by-client”](#) on page 1068
  - [“ip dhcp snooping delete-by-linkdown”](#) on page 1069
  - [“ip dhcp snooping max-bindings”](#) on page 1070

- ["ip dhcp snooping subscriber-id"](#) on page 1071
- ["ip dhcp snooping trust"](#) on page 1072
- ["ip dhcp snooping verify mac-address"](#) on page 1073
- ["ip dhcp snooping violation"](#) on page 1074
- ["ip source binding"](#) on page 1075
- ["service dhcp-snooping"](#) on page 1077
- ["show arp security"](#) on page 1079
- ["show arp security interface"](#) on page 1080
- ["show arp security statistics"](#) on page 1082
- ["show debugging arp security"](#) on page 1085
- ["show debugging ip dhcp snooping"](#) on page 1086
- ["show ip dhcp snooping"](#) on page 1087
- ["show ip dhcp snooping acl"](#) on page 1088
- ["show ip dhcp snooping agent-option"](#) on page 1091
- ["show ip dhcp snooping binding"](#) on page 1094
- ["show ip dhcp snooping interface"](#) on page 1096
- ["show ip dhcp snooping statistics"](#) on page 1098
- ["show ip source binding"](#) on page 1102

# arp security

**Overview** Use this command to enable ARP security on untrusted ports in the VLANs, so that the switch only responds to/forwards ARP packets if they have recognized IP and MAC source addresses.

Use the **no** variant of this command to disable ARP security on the VLANs.

**Syntax** arp security  
no arp security

**Default** Disabled

**Mode** Interface Configuration (VLANs)

**Usage** Enable ARP security to provide protection against ARP spoofing. DHCP snooping must also be enabled on the switch ([service dhcp-snooping](#) command), and on the VLANs ([ip dhcp snooping](#) command).

**Example** To enable ARP security on VLANs 2 to 4, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# arp security
```

**Related Commands** [arp security violation](#)  
[show arp security](#)  
[show arp security interface](#)  
[show arp security statistics](#)

# arp security violation

**Overview** Use this command to specify an additional action to perform if an ARP security violation is detected on the ports. ARP security must also be enabled ([arp security](#) command).

Use the **no** variant of this command to remove the specified action, or all actions. Traffic violating ARP security will be dropped, but no other action will be taken.

**Syntax** `arp security violation {log|trap|link-down} ...`  
`no arp security violation [log|trap|link-down] ...`

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log       | Generate a log message. To display these messages, use the <a href="#">show log</a> command.                                                                                                                                                                                                                                                                                                                                           |
| trap      | Generate an SNMP notification (trap). To send SNMP notifications, SNMP must also be configured, and DHCP snooping notifications must be enabled using the <a href="#">snmp-server enable trap</a> command. Notifications are limited to one per second and to one per source MAC and violation reason. Additional violations within a second of a notification being sent will not result in further notifications. Default: disabled. |
| link-down | Shut down the port that received the packet. Default: disabled.                                                                                                                                                                                                                                                                                                                                                                        |

**Default** When the switch detects an ARP security violation, it drops the packet. By default, it does not perform any other violation actions.

**Mode** Interface Configuration (switch ports, static or dynamic aggregated links)

**Usage** When the switch detects an ARP security violation on an untrusted port in a VLAN that has ARP security enabled, it drops the packet. This command sets the switch to perform additional actions in response to ARP violations.

If a port has been shut down in response to a violation, to bring it back up again after any issues have been resolved, use the [shutdown](#) command.

**Example** To send SNMP notifications for ARP security violations on ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap dhcpsnooping
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# arp security violation trap
```

**Related  
Commands**

- arp security
- show arp security interface
- show arp security statistics
- show log
- snmp-server enable trap

# clear arp security statistics

**Overview** Use this command to clear ARP security statistics for the specified ports, or for all ports.

**Syntax** clear arp security statistics [interface *<port-list>*]

| Parameter                | Description                                                                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | The ports to clear statistics for. If no ports are specified, statistics are cleared for all ports. The ports may be switch ports, or static or dynamic link aggregators. |

**Mode** Privileged Exec

**Example** To clear statistics for ARP security on interface port1.0.1, use the command:  
awplus# clear arp security statistics interface port1.0.1

**Related Commands**

- arp security violation
- show arp security
- show arp security statistics



# clear ip dhcp snooping binding

**Overview** Use this command to remove one or more DHCP Snooping dynamic entries from the DHCP Snooping binding database. If no options are specified, all entries are removed from the database.

**CAUTION:** *If you remove entries from the database for current clients, they will lose IP connectivity until they request and receive a new DHCP lease. If you clear all entries, all clients connected to untrusted ports will lose connectivity.*

**Syntax** `clear ip dhcp snooping binding [<ipaddr>] [interface <port-list>] [vlan <vid-list>]`

| Parameter   | Description                                                                                                                          |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <ipaddr>    | Remove the entry for this client IP address.                                                                                         |
| <port-list> | Remove all entries for these ports. The port list may contain switch ports, and static or dynamic link aggregators (channel groups). |
| <vid-list>  | Remove all entries associated with these VLANs.                                                                                      |

**Mode** Privileged Exec

**Usage** This command removes dynamic entries from the database. Note that dynamic entries can also be deleted by using the **no** variant of the [ip dhcp snooping binding](#) command.

Dynamic entries can individually restored by using the [ip dhcp snooping binding](#) command.

To remove static entries, use the **no** variant of the [ip source binding](#) command.

**Example** To remove a dynamic lease entry from the DHCP snooping database for a client with the IP address 192.168.1.2, use the command:

```
awplus# clear ip dhcp snooping binding 192.168.1.2
```

**Related Commands**

- [ip dhcp snooping binding](#)
- [ip source binding](#)
- [show ip dhcp snooping binding](#)

# clear ip dhcp snooping statistics

**Overview** Use this command to clear DHCP snooping statistics for the specified ports, or for all ports.

**Syntax** `clear ip dhcp snooping statistics [interface <port-list>]`

| Parameter   | Description                                                                                                                                                                        |
|-------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <port-list> | The ports to clear statistics for. If no ports are specified, statistics are cleared for all ports. The port list can contain switch ports, or static or dynamic link aggregators. |

**Mode** Privileged Exec

**Example** To clear statistics for the DHCP snooping on interface port1.0.1, use the command:  
`awplus# clear ip dhcp snooping statistics interface port1.0.1`

**Related Commands**

- [clear arp security statistics](#)
- [show ip dhcp snooping](#)
- [show ip dhcp snooping statistics](#)

# debug arp security

**Overview** Use this command to enable ARP security debugging.  
Use the **no** variant of this command to disable debugging for ARP security.

**Syntax** debug arp security  
no debug arp security

**Default** Disabled

**Mode** Privileged Exec

**Example** To enable ARP security debugging, use the commands:  
awplus# debug arp security

**Related  
Commands** show debugging arp security  
show log  
terminal monitor

# debug ip dhcp snooping

**Overview** Use this command to enable the specified types of debugging for DHCP snooping. Use the **no** variant of this command to disable the specified types of debugging.

**Syntax** debug ip dhcp snooping {all|acl|db|packet [detail]}  
no debug ip dhcp snooping {all|acl|db|packet [detail]}

| Parameter | Description                                                                                                                                |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------|
| all       | All DHCP snooping debug.                                                                                                                   |
| acl       | DHCP snooping access list debug.                                                                                                           |
| db        | DHCP snooping binding database debug.                                                                                                      |
| packet    | DHCP snooping packet debug. For the <b>no</b> variant of this command, this option also disables detailed packet debug, if it was enabled. |
| detail    | Detailed packet debug.                                                                                                                     |

**Default** Disabled

**Mode** Privileged Exec

**Example** To enable access list debugging for DHCP snooping, use the commands:  
awplus# debug ip dhcp snooping acl

**Related Commands** [debug arp security](#)  
[show debugging ip dhcp snooping](#)  
[show log](#)  
[terminal monitor](#)

# ip dhcp snooping

**Overview** Use this command to enable DHCP snooping on one or more VLANs.  
Use the **no** variant of this command to disable DHCP snooping on the VLANs.

**Syntax** ip dhcp snooping  
no ip dhcp snooping

**Default** DHCP snooping is disabled on VLANs by default.

**Mode** Interface Configuration (VLANs)

**Usage** For DHCP snooping to operate on a VLAN, it must:

- be enabled on the particular VLAN by using this command
- be enabled globally on the switch by using the [service dhcp-snooping](#) command
- have at least one port connected to a DHCP server configured as a trusted port by using the [ip dhcp snooping trust](#) command

Any ACLs on a port that permit traffic matching DHCP snooping entries and block other traffic, will block all traffic if DHCP snooping is disabled on the port. If you disable DHCP snooping on particular VLANs using this command, you must also remove any DHCP snooping ACLs from the ports to maintain connectivity (no [access-group](#) command).

**Examples** To enable DHCP snooping on VLANs 2 to 4, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ip dhcp snooping
```

To disable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no ip dhcp snooping
```

**Related Commands** [ip dhcp snooping trust](#)  
[service dhcp-snooping](#)  
[show ip dhcp snooping](#)

# ip dhcp snooping agent-option

**Overview** Use this command to enable DHCP Relay Agent Option 82 information insertion on the switch. When this is enabled, the switch:

- inserts DHCP Relay Agent Option 82 information into DHCP packets that it receives on untrusted ports
- removes DHCP Relay Agent Option 82 information from DHCP packets that it sends to untrusted ports.

Use the **no** variant of this command to disable DHCP Relay Agent Option 82 insertion.

**Syntax** `ip dhcp snooping agent-option`  
`no ip dhcp snooping agent-option`

**Default** DHCP Relay Agent Option 82 insertion is enabled by default when DHCP snooping is enabled.

**Mode** Global Configuration

**Usage** DHCP snooping must also be enabled on the switch ([service dhcp-snooping](#) command), and on the VLANs ([ip dhcp snooping](#) command).

If a subscriber ID is configured for the port ([ip dhcp snooping subscriber-id](#) command), the switch includes this in the DHCP Relay Agent Option 82 information it inserts into DHCP packets received on the port.

**Example** To disable DHCP Relay Agent Option 82 on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping agent-option
```

**Related Commands** [ip dhcp snooping](#)  
[ip dhcp snooping agent-option allow-untrusted](#)  
[ip dhcp snooping subscriber-id](#)  
[service dhcp-snooping](#)  
[show ip dhcp snooping](#)

# ip dhcp snooping agent-option allow-untrusted

**Overview** Use this command to enable DHCP Relay Agent Option 82 information reception on untrusted ports. When this is enabled, the switch accepts incoming DHCP packets that contain DHCP Relay Agent Option 82 information on untrusted ports.

Use the **no** variant of this command to disable DHCP Relay Agent Option 82 information reception on untrusted ports.

**Syntax** `ip dhcp snooping agent-option allow-untrusted`  
`no ip dhcp snooping agent-option allow-untrusted`

**Default** Disabled

**Mode** Global Configuration

**Usage** If the switch is connected via untrusted ports to edge switches that insert DHCP Relay Agent Option 82 information into DHCP packets, you may need to allow these DHCP packets through the untrusted ports, by using this command.

When this is disabled (default), the switch treats incoming DHCP packets on untrusted ports that contain DHCP Relay Agent Option 82 information as DHCP snooping violations: it drops them and applies any violation action specified by the [ip dhcp snooping violation](#) command. The switch stores statistics for packets dropped; to display these statistics, use the [show ip dhcp snooping statistics](#) command.

**Example** To enable DHCP snooping Option 82 information reception on untrusted ports, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping agent-option allow-untrusted
```

**Related Commands** [ip dhcp snooping agent-option](#)  
[ip dhcp snooping violation](#)  
[show ip dhcp snooping](#)  
[show ip dhcp snooping statistics](#)

# ip dhcp snooping agent-option circuit-id vlantriplet

**Overview** Use this command to specify the Circuit ID sub-option of the DHCP Relay Agent Option 82 field as the VLAN ID and port number. The Circuit ID specifies the switch port and VLAN ID that the client-originated DHCP packet was received on.

Use the **no** variant of this command to set the Circuit ID to the default, the VLAN ID and Ifindex (interface number).

**Syntax** `ip dhcp snooping agent-option circuit-id vlantriplet`  
`no ip dhcp snooping agent-option circuit-id`

**Default** By default, the Circuit ID is the VLAN ID and Ifindex (interface number).

**Mode** Interface Configuration for a VLAN interface.

**Usage** The Circuit ID sub-option is included in the DHCP Relay Agent Option 82 field of forwarded client DHCP packets:

- DHCP snooping Option 82 information insertion is enabled ([ip dhcp snooping agent-option](#) command; enabled by default), and
- DHCP snooping is enabled on the switch ([service dhcp-snooping](#)) and on the VLAN to which the port belongs ([ip dhcp snooping](#))

**Examples** To set the Circuit ID to `vlantriplet` for client DHCP packets received on `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp snooping agent-option circuit-id
vlantriplet
```

To return the Circuit ID format to the default for `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp snooping agent-option circuit-id
```

**Related Commands** [ip dhcp snooping agent-option](#)  
[ip dhcp snooping agent-option remote-id](#)  
[show ip dhcp snooping](#)  
[show ip dhcp snooping agent-option](#)



# ip dhcp snooping agent-option remote-id

**Overview** Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field. The Remote ID identifies the device that inserted the Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the switch's MAC address.

Use the **no** variant of this command to set the Remote ID to the default, the switch's MAC address.

**Syntax** `ip dhcp snooping agent-option remote-id <remote-id>`  
`no ip dhcp snooping agent-option remote-id`

| Parameter                      | Description                                                                                                                                                      |
|--------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;remote-id&gt;</code> | An alphanumeric (ASCII) string, 1 to 63 characters in length. If the Remote ID contains spaces, it must be enclosed in double quotes. Wildcards are not allowed. |

**Default** The Remote ID is set to the switch's MAC address by default.

**Mode** Interface Configuration for a VLAN interface.

**Usage** The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of forwarded client DHCP packets:

- DHCP snooping Option 82 information insertion is enabled ([ip dhcp snooping agent-option](#) command; enabled by default), and
- DHCP snooping is enabled on the switch ([service dhcp-snooping](#)) and on the VLAN to which the port belongs ([ip dhcp snooping](#))

**Examples** To set the Remote ID to `myid` for client DHCP packets received on `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp snooping agent-option remote-id myid
```

To return the Remote ID format to the default for `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp snooping agent-option remote-id
```

**Related Commands** [ip dhcp snooping agent-option](#)  
[ip dhcp snooping agent-option circuit-id vlantriplet](#)  
[show ip dhcp snooping](#)  
[show ip dhcp snooping agent-option](#)

# ip dhcp snooping binding

**Overview** Use this command to manually add a dynamic-like entry (with an expiry time) to the DHCP snooping database. Once added to the database, this entry is treated as a dynamic entry, and is stored in the DHCP snooping database backup file. This command is not stored in the switch's running configuration.

Use the **no** variant of this command to delete a dynamic entry for an IP address from the DHCP snooping database, or to delete all dynamic entries from the database.

**CAUTION: If you remove entries from the database for current clients, they will lose IP connectivity until they request and receive a new DHCP lease. If you clear all entries, all clients connected to untrusted ports will lose connectivity.**

**Syntax** `ip dhcp snooping binding <ipaddr> [<macaddr>] vlan <vid>  
interface <port> expiry <expiry-time>  
no ip dhcp snooping binding [<ipaddr>]`

| Parameter     | Description                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------|
| <ipaddr>      | Client's IP address.                                                                                                         |
| <macaddr>     | Client's MAC address in HHHH.HHHH.HHHH format.                                                                               |
| <vid>         | The VLAN ID for the entry, in the range 1 to 4094.                                                                           |
| <port>        | The port the client is connected to. The port can be a switch port, or a static or dynamic link aggregation (channel group). |
| <expiry-time> | The expiry time for the entry, in the range 5 to 2147483647 seconds.                                                         |

**Mode** Privileged Exec

**Usage** Note that dynamic entries can also be deleted from the DHCP snooping database by using the [clear ip dhcp snooping binding](#) command.

To add or remove static entries from the database, use the [ip source binding](#) command.

**Example** To restore an entry in the DHCP snooping database for a DHCP client with the IP address 192.168.1.2, MAC address 0001.0002.0003, on port1.0.6 of vlan6, and with an expiry time of 1 hour, use the commands:

```
awplus# ip dhcp snooping binding 192.168.1.2 0001.0002.0003
vlan 6 interface port1.0.6 expiry 3600
```

**Related Commands** [clear ip dhcp snooping binding](#)  
[ip source binding](#)  
[show ip dhcp snooping binding](#)

# ip dhcp snooping database

**Overview** Use this command to set the location of the file to which the dynamic entries in the DHCP snooping database are written. This file provides a backup for the DHCP snooping database.

Use the **no** variant of this command to set the database location back to the default, **nvs**.

**Syntax** `ip dhcp snooping database {nvs|flash|usb}`  
`no ip dhcp snooping database`

| Parameter | Description                                                                                                                             |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------|
| nvs       | The switch checks the database and writes the file to non-volatile storage (NVS) on the switch at 2 second intervals if it has changed. |
| flash     | The switch checks the database and writes the file to Flash memory on the switch at 60 second intervals if it has changed.              |

**Default** NVS

**Mode** Global Configuration

**Usage** If the location of the backup file is changed by using this command, a new file is created in the new location, and the old version of the file remains in the old location. This can be removed if necessary (hidden file: **.dhcp.dsn.gz**).

**Example** To set the location of the DHCP snooping database to non-volatile storage on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping database nvs
```

**Related Commands** [show ip dhcp snooping](#)

# ip dhcp snooping delete-by-client

**Overview** Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when it receives a valid DHCP release message with matching IP address, VLAN ID, and client hardware address on an untrusted port, and to discard release messages that do not match an entry in the database.

Use the **no** variant of this command to set the switch to forward DHCP release messages received on untrusted ports without removing any entries from the database.

**Syntax** `ip dhcp snooping delete-by-client`  
`no ip dhcp snooping delete-by-client`

**Default** Enabled: by default, DHCP lease entries are deleted from the DHCP snooping database when matching DHCP release messages are received.

**Mode** Global Configuration

**Usage** DHCP clients send a release message when they no longer wish to use the IP address they have been allocated by a DHCP server. Use this command to enable DHCP snooping to use the information in these messages to remove entries from its database immediately. Use the **no** variant of this command to ignore these release messages. Lease entries corresponding to ignored DHCP release messages eventually time out when the lease expires.

**Examples** To set the switch to delete DHCP snooping lease entries from the DHCP snooping database when a matching release message is received, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping delete-by-client
```

To set the switch to forward and ignore the content of any DHCP release messages it receives, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping delete-by-client
```

**Related Commands** [show ip dhcp snooping](#)

# ip dhcp snooping delete-by-linkdown

**Overview** Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when its port goes down. If the port is part of an aggregated link, the entries in the database are only deleted if all the ports in the aggregated link are down.

Use the **no** variant of this command to set the switch not to delete entries when ports go down.

**Syntax** `ip dhcp snooping delete-by-linkdown`  
`no ip dhcp snooping delete-by-linkdown`

**Default** Disabled: by default DHCP Snooping bindings are not deleted when an interface goes down.

**Mode** Global Configuration

**Examples** To set the switch to delete DHCP snooping lease entries from the DHCP snooping database when links go down, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping delete-by-linkdown
```

To set the switch not to delete DHCP snooping lease entries from the DHCP snooping database when links go down, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping delete-by-linkdown
```

**Related Commands** [show ip dhcp snooping](#)

# ip dhcp snooping max-bindings

**Overview** Use this command to set the maximum number of DHCP lease entries that can be stored in the DHCP snooping database for each of the ports. Once this limit has been reached, no further DHCP lease allocations made to devices on the port are stored in the database.

Use the **no** variant of this command to reset the maximum to the default, 1.

**Syntax** `ip dhcp snooping max-bindings <0-520>`  
`no ip dhcp snooping max-bindings`

| Parameter | Description                                                                                                                                                                       |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <0-520>   | The maximum number of bindings that will be stored for the port in the DHCP snooping binding database. If 0 is specified, no entries will be stored in the database for the port. |

**Default** The default for maximum bindings is 1.

**Mode** Interface Configuration (port)

**Usage** The maximum number of leases cannot be changed for a port while there are DHCP snooping Access Control Lists (ACL) associated with the port. Before using this command, remove any DHCP snooping ACLs associated with the ports. To display ACLs used for DHCP snooping, use the [show ip dhcp snooping acl](#) command.

In general, the default (1) will work well on an edge port with a single directly connected DHCP client. If the port is on an aggregation switch that is connected to an edge switch with multiple DHCP clients connected through it, then use this command to increase the number of lease entries for the port.

If there are multiple VLANs configured on the port, the limit is shared between all the VLANs on this port. For example, the default only allows one lease to be stored for one VLAN. To allow connectivity for the other VLANs, use this command to increase the number of lease entries for the port.

**Example** To set the maximum number of bindings to be stored in the DHCP snooping database to 10 per port for ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# ip dhcp snooping max-bindings 10
```

**Related Commands** [access-group](#)  
[show ip dhcp snooping acl](#)  
[show ip dhcp snooping interface](#)

# ip dhcp snooping subscriber-id

**Overview** Use this command to set a Subscriber ID for the ports.  
Use the **no** variant of this command to remove Subscriber IDs from the ports.

**Syntax** `ip dhcp snooping subscriber-id [<sub-id>]`  
`no ip dhcp snooping subscriber-id`

| Parameter | Description                                                                                                                                                                            |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <sub-id>  | The Subscriber ID; an alphanumeric (ASCII) string 1 to 50 characters in length. If the Subscriber ID contains spaces, it must be enclosed in double quotes. Wildcards are not allowed. |

**Default** No Subscriber ID.

**Mode** Interface Configuration (port)

**Usage** The Subscriber ID sub-option is included in the DHCP Relay Agent Option 82 field of client DHCP packets forwarded from a port if:

- a Subscriber ID is specified for the port using this command, and
- DHCP snooping Option 82 information insertion is enabled ([ip dhcp snooping agent-option](#) command; enabled by default), and
- DHCP snooping is enabled on the switch ([service dhcp-snooping](#)) and on the VLAN to which the port belongs ([ip dhcp snooping](#))

**Examples** To set the Subscriber ID for port 1.0.3 to **room\_534**, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# ip dhcp snooping subscriber-id room_534
```

To remove the Subscriber ID from port 1.0.3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no ip dhcp snooping subscriber-id
```

**Related Commands** [ip dhcp snooping agent-option](#)  
[show ip dhcp snooping interface](#)

# ip dhcp snooping trust

**Overview** Use this command to set the ports to be DHCP snooping trusted ports.  
Use the **no** variant of this command to return the ports to their default as untrusted ports.

**Syntax** ip dhcp snooping trust  
no ip dhcp snooping trust

**Default** All ports are untrusted by default.

**Mode** Interface Configuration (port)

**Usage** Typically, ports connecting the switch to trusted elements in the network (towards the core) are set as trusted ports, while ports connecting untrusted network elements are set as untrusted. Configure ports connected to DHCP servers as trusted ports.

**Example** To set switch ports 1.0.1 and 1.0.2 to be trusted ports, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# ip dhcp snooping trust
```

**Related Commands** [show ip dhcp snooping interface](#)



# ip dhcp snooping verify mac-address

**Overview** Use this command to verify that the source MAC address and client hardware address match in DHCP packets received on untrusted ports.

Use the **no** variant of this command to disable MAC address verification.

**Syntax** `ip dhcp snooping verify mac-address`  
`no ip dhcp snooping verify mac-address`

**Default** Enabled—source MAC addresses are verified by default.

**Mode** Global Configuration

**Usage** When MAC address verification is enabled, the switch treats DHCP packets with source MAC address and client hardware address that do not match as DHCP snooping violations: it drops them and applies any other violation action specified by the [ip dhcp snooping violation](#) command. To bring the port back up again after any issues have been resolved, use the [shutdown](#) command.

**Example** To disable MAC address verification on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping verify mac-address
```

**Related Commands** [ip dhcp snooping violation](#)  
[show ip dhcp snooping](#)  
[show ip dhcp snooping statistics](#)

# ip dhcp snooping violation

**Overview** Use this command to specify the action the switch will take when it detects a DHCP snooping violation by a DHCP packet on the ports.

Use the **no** variant of this command to disable the specified violation actions, or all violation actions.

**Syntax** `ip dhcp snooping violation {log|trap|link-down} ...`  
`no ip dhcp snooping violation [{log|trap|link-down} ...]`

| Parameter | Description                                                                                                                                                                                                                                                                                                                  |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log       | Generate a log message. To display these messages, use the <a href="#">show log</a> command.<br>Default: disabled.                                                                                                                                                                                                           |
| trap      | Generate an SNMP notification (trap). To send SNMP notifications, SNMP must also be configured, and DHCP snooping notifications must be enabled using the <a href="#">snmp-server enable trap</a> command. Notifications are limited to one per second and to one per source MAC and violation reason.<br>Default: disabled. |
| link-down | Set the port status to link-down.<br>Default: disabled.                                                                                                                                                                                                                                                                      |

**Default** By default, DHCP packets that violate DHCP snooping are dropped, but no other violation action is taken.

**Mode** Interface Configuration (port)

**Usage** If a port has been shut down in response to a violation, to bring it back up again after any issues have been resolved, use the [shutdown](#) command.

IP packets dropped by DHCP snooping filters do not result in other DHCP snooping violation actions.

**Example** To set the switch to send an SNMP notification and set the link status to link-down if it detects a DHCP snooping violation on switch ports 1.0.1 to 1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap dhcpsnooping
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# ip dhcp snooping violation trap link-down
```

**Related Commands** [show ip dhcp snooping interface](#)  
[show log](#)  
[snmp-server enable trap](#)

# ip source binding

**Overview** Use this command to add or replace a static entry in the DHCP snooping database. Use the **no** variant of this command to delete the specified static entry or all static entries from the database.

**Syntax** `ip source binding <ipaddr> [<macaddr>] vlan <vid> interface <port>`  
`no ip source binding [<ipaddr>]`

| Parameter | Description                                                                                                                                            |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ipaddr>  | Client's IP address. If there is already an entry in the DHCP snooping database for this IP address, then this command replaces it with the new entry. |
| <macaddr> | Client's MAC address in HHHH.HHHH.HHHH format.                                                                                                         |
| <vid>     | The VLAN ID associated with the entry.                                                                                                                 |
| <port>    | The port the client is connected to.                                                                                                                   |

**Mode** Global Configuration

**Usage** This command removes static entries from the database. To remove dynamic entries, use the [clear ip dhcp snooping binding](#) command or the **no** variant of the [ip dhcp snooping binding](#) command.

**Examples** To add a static entry to the DHCP snooping database for a client with the IP address 192.168.1.2, MAC address 0001.0002.0003, on port1.0.6 of vlan6, use the command:

```
awplus# configure terminal
awplus(config)# ip source binding 192.168.1.2 0001.0002.0003
vlan 6 interface port1.0.6
```

To remove the static entry for IP address 192.168.1.2 from the database, use the commands:

```
awplus# configure terminal
awplus(config)# no ip source binding 192.168.1.2
```

To remove all static entries from the database, use the commands:

```
awplus# configure terminal
awplus(config)# no ip source binding
```

**Related  
Commands**

- [clear ip dhcp snooping binding](#)
- [ip dhcp snooping binding](#)
- [show ip dhcp snooping binding](#)
- [show ip source binding](#)

# service dhcp-snooping

**Overview** Use this command to enable the DHCP snooping service globally on the switch. This must be enabled before other DHCP snooping configuration commands can be entered.

Use the **no** variant of this command to disable the DHCP snooping service on the switch. This removes all DHCP snooping configuration from the running configuration, except for any DHCP snooping maximum bindings settings ([ip dhcp snooping max-bindings](#) command), and any DHCP snooping-based Access Control Lists (ACLs), which are retained when the service is disabled.

**Syntax** service dhcp-snooping  
no service dhcp-snooping

**Default** DHCP snooping is disabled on the switch by default.

**Mode** Global Configuration

**Usage** For DHCP snooping to operate on a VLAN, it must be enabled on the switch by using this command, and also enabled on the particular VLAN by using the [ip dhcp snooping](#) command.

For DHCP snooping to operate on a VLAN, it must:

- be enabled globally on the switch by using this command
- be enabled on the particular VLAN by using the [ip dhcp snooping](#) command
- have at least one port connected to a DHCP server configured as a trusted port by using the [ip dhcp snooping trust](#) command

If you disable the DHCP snooping service by using the **no** variant of this command, all DHCP snooping configuration (including ARP security, but excluding maximum bindings and ACLs) is removed from the running configuration, and the DHCP snooping database is deleted from active memory. If you re-enable the service, the switch repopulates the DHCP snooping database from the dynamic lease entries in the database backup file (in NVS by default—see the [ip dhcp snooping database](#) command). The lease expiry times are updated.

The DHCP snooping service cannot be enabled on a switch that is configured with any of the following features, or vice versa:

- web authentication ([auth-web enable](#) command)
- roaming authentication ([auth roaming enable](#) command, [auth roaming disconnected](#) command)
- guest VLAN authentication ([auth guest-vlan](#) command).

Any ACLs on a port that permit traffic matching DHCP snooping entries and block other traffic, will block all traffic if DHCP snooping is disabled on the port. If you disable DHCP snooping on the switch using this command, you must also remove any DHCP snooping ACLs from the ports to maintain connectivity ([no access-group](#) command).

**Examples** To enable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# service dhcp-snooping
```

To disable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# no service dhcp-snooping
```

**Related  
Commands**

- [ip dhcp snooping](#)
- [ip dhcp snooping database](#)
- [ip dhcp snooping max-bindings](#)
- [show ip dhcp snooping](#)

# show arp security

**Overview** Use this command to display ARP security configuration.

**Syntax** show arp security

**Mode** User Exec and Privileged Exec

**Example** To display ARP security configuration on the switch use the command:

```
awplus# show arp security
```

Table 33-1: Example output from the **show arp security** command

```
awplus# show arp security

ARP Security Information:
 Total VLANs enabled 2
 Total VLANs disabled 11
 vlan1 Disabled
 vlan2 Disabled
 vlan3 Disabled
 vlan4 Disabled
 vlan5 Disabled
 vlan100 Disabled
 vlan101 Disabled
 vlan102 Disabled
 vlan103 Disabled
 vlan104 Disabled
 vlan105 Enabled
 vlan1000 Disabled
 vlan1001 Enabled
```

Table 33-2: Parameters in the output from the **show arp security** command

| Parameter            | Description                                          |
|----------------------|------------------------------------------------------|
| Total VLANs enabled  | The number of VLANs that have ARP security enabled.  |
| Total VLANs disabled | The number of VLANs that have ARP security disabled. |

**Related Commands**

- [arp security](#)
- [show arp security interface](#)
- [show arp security statistics](#)

# show arp security interface

**Overview** Use this command to display ARP security configuration for the specified ports or all ports.

**Syntax** show arp security interface [*<port-list>*]

| Parameter                | Description                                                                                                                          |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | The ports to display ARP security information about. The port list can include switch ports, and static or dynamic aggregated links. |

**Mode** User Exec and Privileged Exec

**Example** To display ARP security configuration for ports, use the command:

```
awplus# show arp security interface
```

Table 33-3: Example output from the **show arp security interface** command

|                                                                |          |
|----------------------------------------------------------------|----------|
| awplus#show arp security interface                             |          |
| Arp Security Port Status and Configuration:                    |          |
| Port: Provisioned ports marked with brackets, e.g. (portx.y.z) |          |
| KEY: LG = Log                                                  |          |
| TR = Trap                                                      |          |
| LD = Link down                                                 |          |
| Port                                                           | Action   |
| -----                                                          |          |
| port1.0.1                                                      | -- -- -- |
| port1.0.2                                                      | -- -- -- |
| port1.0.3                                                      | LG TR LD |
| port1.0.4                                                      | LG -- -- |
| port1.0.5                                                      | LG -- -- |
| port1.0.6                                                      | LG TR -- |

Table 33-4: Parameters in the output from the **show arp security interface** command

| Parameter | Description                                                                        |
|-----------|------------------------------------------------------------------------------------|
| Action    | The action the switch takes when it detects an ARP security violation on the port. |
| Port      | The port. Parentheses indicate that ports are configured for provisioning.         |
| LG, Log   | Generate a log message                                                             |



Table 33-4: Parameters in the output from the **show arp security interface** command (cont.)

| Parameter     | Description                           |
|---------------|---------------------------------------|
| TR, Trap      | Generate an SNMP notification (trap). |
| LD, Link down | Shut down the link.                   |

**Related  
Commands**

- [arp security violation](#)
- [show arp security](#)
- [show arp security statistics](#)
- [show log](#)
- [snmp-server enable trap](#)

# show arp security statistics

**Overview** Use this command to display ARP security statistics for the specified ports or all ports.

**Syntax** `show arp security statistics [detail] [interface <port-list>]`

| Parameter                                | Description                                 |
|------------------------------------------|---------------------------------------------|
| <code>detail</code>                      | Display detailed statistics.                |
| <code>interface &lt;port-list&gt;</code> | Display statistics for the specified ports. |

**Mode** User Exec and Privileged Exec

**Example** To display the brief statistics for the ARP security, use the command:

```
awplus# show arp security statistics
```

Table 33-5: Example output from the **show arp security statistics** command

```
awplus# show arp security statistics
```

| DHCP Snooping ARP Security Statistics: |               |                |
|----------------------------------------|---------------|----------------|
| Interface                              | In<br>Packets | In<br>Discards |
| -----                                  |               |                |
| port1.0.3                              | 20            | 20             |
| port1.0.4                              | 30            | 30             |

Table 33-6: Parameters in the output from the **show arp security statistics** command

| Parameter   | Description                                                                               |
|-------------|-------------------------------------------------------------------------------------------|
| Interface   | A port name. Parentheses indicate that ports are configured for provisioning.             |
| In Packets  | The total number of incoming ARP packets that are processed by DHCP Snooping ARP Security |
| In Discards | The total number of ARP packets that are dropped by DHCP Snooping ARP Security.           |

Table 33-7: Example output from the **show arp security statistics detail** command

```
awplus#show arp security statistics detail
```

| DHCP Snooping ARP Security Statistics: |           |
|----------------------------------------|-----------|
| Interface .....                        | port1.0.3 |
| In Packets .....                       | 20        |
| In Discards .....                      | 20        |
| No Lease .....                         | 20        |
| Bad Vlan .....                         | 0         |
| Bad Port .....                         | 0         |
| Source Ip Not Allocated ....           | 0         |
| Interface .....                        | port1.0.4 |
| In Packets .....                       | 30        |
| In Discards .....                      | 30        |
| No Lease .....                         | 30        |
| Bad Vlan .....                         | 0         |
| Bad Port .....                         | 0         |
| Source Ip Not Allocated ....           | 0         |

**Related  
Commands**

- arp security
- arp security violation
- clear arp security statistics
- show arp security
- show arp security interface
- show log

# show debugging arp security

**Overview** Use this command to display the ARP security debugging configuration.

**Syntax** show debugging arp security

**Mode** User and Privileged Exec

**Example** To display the debugging settings for ARP security on the switch, use the command:

```
awplus# show debugging arp security
```

Table 33-8: Example output from the **show debugging arp security** command

```
awplus# show debugging arp security

ARP Security debugging status:
 ARP Security debugging is off
```

**Related  
Commands** [arp security violation](#)  
[debug arp security](#)

# show debugging ip dhcp snooping

**Overview** Use this command to display the DHCP snooping debugging configuration.

**Syntax** show debugging ip dhcp snooping

**Mode** User Exec and Privileged Exec

**Example** To display the DHCP snooping debugging configuration, use the command:

```
awplus# show debugging ip dhcp snooping
```

Table 33-9: Example output from the **show debugging ip dhcp snooping** command

```
awplus# show debugging ip dhcp snooping

DHCP snooping debugging status:
 DHCP snooping debugging is off
 DHCP snooping all debugging is off
 DHCP snooping acl debugging is off
 DHCP snooping binding DB debugging is off
 DHCP snooping packet debugging is off
 DHCP snooping detailed packet debugging is off
```

**Related Commands** [debug ip dhcp snooping](#)  
[show log](#)

# show ip dhcp snooping

**Overview** Use this command to display DHCP snooping global configuration on the switch.

**Syntax** show ip dhcp snooping

**Mode** User Exec and Privileged Exec

**Example** To display global DHCP snooping configuration on the switch, use the command:

```
awplus# show ip dhcp snooping
```

Table 33-10: Example output from the **show ip dhcp snooping** command

```
DHCP Snooping Information:
 DHCP Snooping service Enabled

Option 82 insertion Enabled

Option 82 on untrusted ports Not allowed
 Binding delete by client Disabled
 Binding delete by link down Disabled
 Verify MAC address Disabled
 SNMP DHCP Snooping trap Disabled

DHCP Snooping database:
 Database location nvs Number of entries in
 database 2

DHCP Snooping VLANs:
 Total VLANs enabled 1
 Total VLANs disabled 9
 vlan1 Enabled
 vlan2 Disabled
 vlan3 Disabled
 vlan4 Disabled
 vlan5 Disabled
 vlan100 Disabled
 vlan101 Disabled
 vlan105 Disabled
 vlan1000 Disabled
 vlan1001 Disabled
```

**Related Commands**

- [service dhcp-snooping](#)
- [show arp security](#)
- [show ip dhcp snooping acl](#)
- [show ip dhcp snooping agent-option](#)
- [show ip dhcp snooping binding](#)
- [show ip dhcp snooping interface](#)

# show ip dhcp snooping acl

**Overview** Use this command to display information about the Access Control Lists (ACL) that are using the DHCP snooping database.

**Syntax** show ip dhcp snooping acl  
show ip dhcp snooping acl [detail|hardware] [interface  
[<interface-list>]]

| Parameter        | Description                                  |
|------------------|----------------------------------------------|
| detail           | Detailed DHCP Snooping ACL information.      |
| hardware         | DHCP Snooping hardware ACL information.      |
| interface        | ACL Interface information.                   |
| <interface-list> | The interfaces to display information about. |

**Mode** User Exec and Privileged Exec

**Example** To display DHCP snooping ACL information, use the command:

```
awplus# show ip dhcp snooping acl
```

Table 33-11: Example output from the **show ip dhcp snooping acl** command

| awplus#show ip dhcp snooping acl     |          |                  |                  |                           |
|--------------------------------------|----------|------------------|------------------|---------------------------|
| DHCP Snooping Based Filters Summary: |          |                  |                  |                           |
| Interface                            | Bindings | Maximum Bindings | Template Filters | Attached Hardware Filters |
| -----                                |          |                  |                  |                           |
| -                                    |          |                  |                  |                           |
| port1.0.1                            | 1        | 520              | 0                | 0                         |
| port1.0.2                            | 1        | 3                | 2                | 6                         |
| port1.0.3                            | 1        | 2                | 4                | 8                         |
| port1.0.4                            | 1        | 2                | 7                | 14                        |
| port1.0.5                            | 0        | 2                | 6                | 12                        |
| port1.0.6                            | 0        | 1                | 0                | 0                         |



To display DHCP snooping hardware ACL information, use the command:

```
awplus# show ip dhcp snooping acl hardware
```

Table 33-12: Example output from the **show ip dhcp snooping acl hardware** command

```
awplus#show ip dhcp snooping acl hardware
```

DHCP Snooping Based Filters in Hardware:

| Interface | Access-list(/ClassMap) | Source IP   | Source MAC     |
|-----------|------------------------|-------------|----------------|
| port1.0.2 | dhcpsn1                | 10.10.10.10 | aaaa.bbbb.cccc |
| port1.0.2 | dhcpsn1                | 20.20.20.20 | 0000.aaaa.bbbb |
| port1.0.2 | dhcpsn1                | 0.0.0.0     | 0000.0000.0000 |
| port1.0.2 | dhcpsn1                | 0.0.0.0     | 0000.0000.0000 |
| port1.0.2 | dhcpsn1                | 0.0.0.0     | 0000.0000.0000 |
| port1.0.2 | dhcpsn1                | 0.0.0.0     | 0000.0000.0000 |
| port1.0.3 | dhcpsn2/cmap1          | 30.30.30.30 | aaaa.bbbb.dddd |
| port1.0.3 | dhcpsn2/cmap1          | 40.40.40.40 | 0000.aaaa.cccc |
| port1.0.3 | dhcpsn2/cmap1          | 50.50.50.50 | 0000.aaaa.dddd |
| port1.0.3 | dhcpsn2/cmap1          | 60.60.60.60 | 0000.aaaa.eeee |
| port1.0.3 | dhcpsn2/cmap1          | 0.0.0.0     | 0000.0000.0000 |
| port1.0.3 | dhcpsn2/cmap1          | 0.0.0.0     | 0000.0000.0000 |
| port1.0.3 | dhcpsn2/cmap1          | 0.0.0.0     | 0000.0000.0000 |
| port1.0.3 | dhcpsn2/cmap1          | 0.0.0.0     | 0000.0000.0000 |
| port1.0.4 | dhcpsn3/cmap2          | 70.70.70.70 |                |
| port1.0.4 | dhcpsn3/cmap2          | 80.80.80.80 |                |
| port1.0.4 | dhcpsn2/cmap1          | 70.70.70.70 |                |
| port1.0.4 | dhcpsn2/cmap1          | 80.80.80.80 |                |
| port1.0.4 | dhcpsn1                | 70.70.70.70 |                |
| port1.0.4 | dhcpsn1                | 80.80.80.80 |                |

To display detailed DHCP snooping ACL information for port 1.0.4, use the command:

```
awplus# show ip dhcp snooping acl detail interface port1.0.4
```

Table 33-13: Example output from the **show ip dhcp snooping acl detail interface** command

```
awplus#show ip dhcp snooping acl detail interface port1.0.4

DHCP Snooping Based Filters Information:

port1.0.4 : Maximum Bindings 2
port1.0.4 : Template filters 7
port1.0.4 : Attached hardware filters .. 14
port1.0.4 : Current bindings 1, 1 free
port1.0.4 Client 1 120.120.120.120
port1.0.4 : Templates: cheese (via class-map: cmap2)
port1.0.4 : 10 permit ip dhcpsnooping 100.0.0.0/8
port1.0.4 : Template: dhcpsn2 (via class-map: cmap1)
port1.0.4 : 10 permit ip dhcpsnooping any
port1.0.4 : 20 permit ip dhcpsnooping 10.0.0.0/8
port1.0.4 : 30 permit ip dhcpsnooping 20.0.0.0/8
port1.0.4 : 40 permit ip dhcpsnooping 30.0.0.0/8
port1.0.4 : Template: dhcpsn1 (via access-group)
port1.0.4 : 10 permit ip dhcpsnooping any mac dhcpsnooping abcd.0000.0000 00
00.ffff.ffff
port1.0.4 : 20 permit ip dhcpsnooping any
```

**Related  
Commands**    [access-list hardware \(named\)](#)  
              [show access-list \(IPv4 Hardware ACLs\)](#)

# show ip dhcp snooping agent-option

**Overview** Use this command to display DHCP snooping Option 82 information for all interfaces, a specific interface or a range of interfaces.

**Syntax** `show ip dhcp snooping agent-option [interface <interface-list>]`

| Parameter        | Description                                   |
|------------------|-----------------------------------------------|
| interface        | Specify the interface.                        |
| <interface-list> | The name of the interface or interface range. |

**Mode** User Exec and Privileged Exec

**Examples** To display DHCP snooping Option 82 information for all interfaces, use the command:

```
awplus# show ip dhcp snooping agent-option
```

To display DHCP snooping Option 82 information for port1.0.1, use the command:

```
awplus# show ip dhcp snooping agent-option interface port1.0.1
```

To display DHCP snooping Option 82 information for vlan1, use the command:

```
awplus# show ip dhcp snooping agent-option interface vlan1
```

**Output** Figure 33-1: Example output from the **show ip dhcp snooping agent-option** command

```
awplus#show ip dhcp snooping agent-option

DHCP Snooping Option 82 Configuration:

Key: C Id = Circuit Id Format
 R Id = Remote Id
 S Id = Subscriber Id

Option 82 insertion Enabled
Option 82 on untrusted ports Not allowed

vlan1 C Id = vlanifindex
 R Id = Access-Island-01-M1
vlan2 C Id = vlantriplet
 R Id = Access-Island-01-M1
vlan3 C Id = vlantriplet
 R Id = Access-Island-01-M3
vlan4 C Id = vlantriplet
 R Id = 0000.cd28.074c
vlan5 C Id = vlantriplet
 R Id = 0000.cd28.074c
vlan6 C Id = vlantriplet
 R Id = 0000.cd28.074c
port1.0.1 S Id =
port1.0.2 S Id =
port1.0.3 S Id = phone_1
port1.0.4 S Id =
port1.0.5 S Id = PC_1
port1.0.6 S Id = phone_2
```

```
awplus#show ip dhcp snooping agent-option

DHCP Snooping Option 82 Configuration:

Key: C Id = Circuit Id Format
 R Id = Remote Id
 S Id = Subscriber Id

Option 82 insertion Enabled
Option 82 on untrusted ports Not allowed

vlan1 C Id = vlanifindex
 R Id = Access-Island-01-M1
vlan2 C Id = vlantriplet
 R Id = Access-Island-01-M1
vlan3 C Id = vlantriplet
 R Id = Access-Island-01-M3
vlan4 C Id = vlantriplet
 R Id = 0000.cd28.074c
vlan5 C Id = vlantriplet
 R Id = 0000.cd28.074c
vlan6 C Id = vlantriplet
 R Id = 0000.cd28.074c
port1.1.1 S Id =
port1.1.2 S Id =
port1.1.3 S Id = phone_1
port1.1.4 S Id =
port1.1.5 S Id =
port1.1.6 S Id = phone_2
port1.1.7 S Id = PC_1
port1.1.8 S Id =
port1.1.9 S Id =
port1.1.10 S Id =
port1.1.11 S Id =
port1.1.12 S Id =
```

**Related  
Commands**

[ip dhcp snooping agent-option](#)  
[ip dhcp snooping agent-option circuit-id vlantriplet](#)  
[ip dhcp snooping agent-option remote-id](#)  
[ip dhcp snooping subscriber-id](#)  
[show ip dhcp snooping](#)  
[show ip dhcp snooping interface](#)

# show ip dhcp snooping binding

**Overview** Use this command to display all dynamic and static entries in the DHCP snooping binding database.

**Syntax** show ip dhcp snooping binding

**Mode** User Exec and Privileged Exec

**Example** To display entries in the DHCP snooping database, use the command:

```
awplus# show ip dhcp snooping binding
```

Table 33-14: Example output from the **show ip dhcp snooping binding** command

| awplus# show ip dhcp snooping binding<br>DHCP Snooping Bindings: |                |                      |      |       |                  |      |
|------------------------------------------------------------------|----------------|----------------------|------|-------|------------------|------|
| Client<br>IP Address                                             | MAC<br>Address | Server<br>IP Address | VLAN | Port  | Expires<br>(sec) | Type |
| 1.2.3.4                                                          | aaaa.bbbb.cccc | --                   | 7    | 1.0.6 | Infinite         | Stat |
| 1.2.3.6                                                          | any            | --                   | 4077 | 1.0.6 | Infinite         | Stat |
| 1.3.4.5                                                          | any            | --                   | 1    | sa1   | Infinite         | Stat |
| 111.111.100.101                                                  | 0000.0000.0001 | 111.112.1.1          | 1    | 1.0.6 | 4076             | Dyna |
| 111.111.101.108                                                  | 0000.0000.0108 | 111.112.1.1          | 1    | 1.0.6 | 4084             | Dyna |
| 111.111.101.109                                                  | 0000.0000.0109 | 111.112.1.1          | 1    | 1.0.6 | 4085             | Dyna |
| 111.211.100.101                                                  | --             | --                   | 1    | 1.0.2 | 2147483325       | Dyna |
| 111.211.100.109                                                  | 00b0.0000.0009 | 111.112.111.111      | 1    | 1.0.2 | 21               | Dyna |
| 111.211.101.101                                                  | 00b0.0000.0101 | 111.112.111.111      | 1    | 1.0.2 | 214              | Dyna |
| Total number of bindings in database: 9                          |                |                      |      |       |                  |      |

Table 33-15: Parameters in the output from the **show ip dhcp snooping binding** command

| Parameter        | Description                                  |
|------------------|----------------------------------------------|
| Client IPAddress | The IP address of the DHCP client.           |
| MAC Address      | The MAC address of the DHCP client.          |
| Server IP        | The IP address of the DHCP server.           |
| VLAN             | The VLAN associated with this entry.         |
| Port             | The port the client is connected to.         |
| Expires (sec)    | The time in seconds until the lease expires. |

Table 33-15: Parameters in the output from the **show ip dhcp snooping binding** command (cont.)

| Parameter                            | Description                                                                                                                                                                                                                                                                                                                   |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type                                 | The source of the entry: <ul style="list-style-type: none"><li>• Dyna: dynamically entered by snooping DHCP traffic, configured by the <a href="#">ip dhcp snooping binding</a> command, or loaded from the database backup file.</li><li>• Stat: added statically by the <a href="#">ip source binding</a> command</li></ul> |
| Total number of bindings in database | The total number of dynamic and static lease entries in the DHCP snooping database.                                                                                                                                                                                                                                           |

**Related Commands**

- [ip dhcp snooping binding](#)
- [ip dhcp snooping max-bindings](#)
- [show ip source binding](#)

# show ip dhcp snooping interface

**Overview** Use this command to display information about DHCP snooping configuration and leases for the specified ports, or all ports.

**Syntax** show ip dhcp snooping interface [*<port-list>*]

| Parameter                | Description                                                                                                                          |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | The ports to display DHCP snooping configuration information for. If no ports are specified, information for all ports is displayed. |

**Mode** User Exec and Privileged Exec

**Example** To display DHCP snooping information for all ports, use the command:

```
awplus# show ip dhcp snooping interface
```

Table 33-16: Example output from the **show ip dhcp snooping interface** command

| awplus#show ip dhcp snooping interface                         |           |             |            |          |                    |  |
|----------------------------------------------------------------|-----------|-------------|------------|----------|--------------------|--|
| DHCP Snooping Port Status and Configuration:                   |           |             |            |          |                    |  |
| Port: Provisioned ports marked with brackets, e.g. (portx.y.z) |           |             |            |          |                    |  |
| Action: LG = Log                                               |           |             |            |          |                    |  |
| TR = Trap                                                      |           |             |            |          |                    |  |
| LD = Link down                                                 |           |             |            |          |                    |  |
| Port                                                           | Status    | Full Leases | Max Leases | Action   | Subscriber-ID      |  |
| port1.0.1                                                      | Untrusted | 1           | 1          | LG -- -- |                    |  |
| port1.0.2                                                      | Untrusted | 0           | 50         | LG TR LD | Building 1 Level 1 |  |
| port1.0.3                                                      | Untrusted | 0           | 50         | LG -- -- |                    |  |
| port1.0.4                                                      | Untrusted | 0           | 50         | LG -- -- | Building 1 Level 2 |  |
| port1.0.5                                                      | Trusted   | 0           | 1          | -- -- -- |                    |  |
| port1.0.6                                                      | Trusted   | 0           | 1          | -- -- -- |                    |  |

Table 33-17: Parameters in the output from the **show ip dhcp snooping interface** command

| Parameter   | Description                                                       |
|-------------|-------------------------------------------------------------------|
| Port        | The port interface name.                                          |
| Status      | The port status: untrusted (default) or trusted.                  |
| Full Leases | The number of entries in the DHCP snooping database for the port. |



Table 33-17: Parameters in the output from the **show ip dhcp snooping interface** command (cont.)

| Parameter     | Description                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Leases    | The maximum number of entries that can be stored in the database for the port.                                                                                                                                               |
| Action        | The DHCP snooping violation actions for the port.                                                                                                                                                                            |
| Subscriber ID | The subscriber ID for the port. If the subscriber ID is longer than 34 characters, only the first 34 characters are displayed. To display the whole subscriber ID, use the <a href="#">show running-config dhcp</a> command. |

**Related Commands**

- [show ip dhcp snooping](#)
- [show ip dhcp snooping statistics](#)
- [show running-config dhcp](#)

# show ip dhcp snooping statistics

**Overview** Use this command to display DHCP snooping statistics.

**Syntax** show ip dhcp snooping statistics [detail] [interface <interface-list>]

| Parameter                     | Description                                                                                                                                                  |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| detail                        | Display detailed statistics.                                                                                                                                 |
| interface<br><interface-list> | Display statistics for the specified interfaces. The interface list can contain switch ports, static or dynamic link aggregators (channel groups), or VLANs. |

**Mode** User Exec and Privileged Exec

**Example** To show the current DHCP snooping statistics for all interfaces, use the command:

```
awplus# show ip dhcp snooping statistics
```

Table 33-18: Example output from the **show ip dhcp snooping statistics** command

```
awplus# show ip dhcp snooping statistics
```

| DHCP Snooping Statistics: |                     |                      |               |                |
|---------------------------|---------------------|----------------------|---------------|----------------|
| Interface                 | In BOOTP<br>Packets | In BOOTP<br>Requests | In<br>Replies | In<br>Discards |
| vlan1                     | 444                 | 386                  | 58            | 223            |
| port1.0.1                 | 386                 | 386                  | 0             | 223            |
| port1.0.2                 | 0                   | 0                    | 0             | 0              |
| port1.0.3                 | 0                   | 0                    | 0             | 0              |
| port1.0.4                 | 0                   | 0                    | 0             | 0              |
| port1.0.5                 | 0                   | 0                    | 0             | 0              |
| port1.0.6                 | 58                  | 0                    | 58            | 0              |

Table 33-19: Example output from the **show ip dhcp snooping statistics detail** command

```
awplus# show ip dhcp snooping statistics detail
```

| DHCP Snooping Statistics:                  |                           |
|--------------------------------------------|---------------------------|
| Interface .....                            | port1.0.1, All counters 0 |
| Interface .....                            | port1.0.2, All counters 0 |
| Interface .....                            | port1.0.3, All counters 0 |
| Interface .....                            | port1.0.4                 |
| In Packets .....                           | 50                        |
| In BOOTP Requests .....                    | 25                        |
| In BOOTP Replies .....                     | 25                        |
| In Discards .....                          | 1                         |
| Invalid BOOTP Information .....            | 0                         |
| Invalid DHCP ACK .....                     | 0                         |
| Invalid DHCP Release or Decline .....      | 0                         |
| Invalid IP/UDP Header .....                | 0                         |
| Max Bindings Exceeded .....                | 1                         |
| Option 82 Insert Error .....               | 0                         |
| Option 82 Received Invalid .....           | 0                         |
| Option 82 Received On Untrusted Port ..... | 0                         |
| Option 82 Transmit On Untrusted Port ..... | 0                         |
| Reply Received On Untrusted Port .....     | 0                         |
| Source MAC/CHADDR Mismatch .....           | 0                         |
| Static Entry Already Exists .....          | 0                         |
| Interface .....                            | port1.0.5, All counters 0 |
| Interface .....                            | port1.0.6, All counters 0 |

Table 33-20: Parameters in the output from the **show ip dhcp snooping statistics** command

| Parameter                            | Description                                                                                                                               |
|--------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| Interface                            | The interface name.                                                                                                                       |
| In Packets                           | The total number of incoming packets that are processed by DHCP Snooping.                                                                 |
| In BOOTP Requests                    | The total number of incoming BOOTP Requests.                                                                                              |
| In BOOTP Replies                     | The total number of incoming BOOTP Replies.                                                                                               |
| In Discards                          | The total number of incoming packets that have been discarded.                                                                            |
| Invalid BOOTP Information            | Packet contained invalid BOOTP information, such as an invalid BOOTP.OPCode.                                                              |
| Invalid DHCP ACK                     | A DHCP ACK message was discarded, for reasons such as missing Server Option or Lease Option.                                              |
| Invalid DHCP Release or Decline      | A DHCP Release or Decline message was discarded, for reasons such as mismatch between received interface and current binding information. |
| Invalid IP/UDP Header                | A problem was detected in the IP or UDP header of the packet.                                                                             |
| Max Bindings Exceeded                | Accepting the packet would cause the maximum number of bindings on a port to be exceeded.                                                 |
| Option 82 Insert Error               | An error occurred while trying to insert DHCP Relay Agent Option 82 information.                                                          |
| Option 82 Received Invalid           | The DHCP Relay Agent Option 82 information received did not match the information inserted by DHCP Snooping.                              |
| Option 82 Received On Untrusted Port | A packet containing DHCP Relay Agent Option 82 information was received on an untrusted port.                                             |
| Option 82 Transmit On Untrusted Port | A packet containing DHCP Relay Agent Option 82 information was to be sent on an untrusted port.                                           |
| Reply Received On Untrusted Port     | A BOOTP reply was received on an untrusted port.                                                                                          |
| Source MAC/CHADDR Mismatch           | The L2 Source MAC address of the packet did not match the client hardware address field (BOOTP.CHADDR).                                   |
| Static Entry Already Exists          | An entry could not be added as a static entry already exists.                                                                             |

**Related  
Commands**    clear ip dhcp snooping statistics  
                  ip dhcp snooping  
                  ip dhcp snooping violation

# show ip source binding

**Overview** Use this command to display static entries in the DHCP snooping database. These are the entries that have been added by using the [ip source binding](#) command.

**Syntax** show ip source binding

**Mode** User Exec and Privileged Exec

**Example** To display static entries in the DHCP snooping database information, use the command:

```
awplus# show ip source binding
```

Table 33-21: Example output from the **show ip source binding** command

|                                |                |       |           |                  |        |       |
|--------------------------------|----------------|-------|-----------|------------------|--------|-------|
| awplus# show ip source binding |                |       |           |                  |        |       |
| IP Source Bindings:            |                |       |           |                  |        |       |
| Client<br>IP Address           | MAC<br>Address | VLAN  | Port      | Expires<br>(sec) | Type   |       |
| -----                          | -----          | ----- | -----     | -----            | -----  | ----- |
| 1.1.1.1                        | 0000.1111.2222 | 1     | port1.0.1 | Infinite         | Static |       |

Table 33-22: Parameters in the output from the **show ip source binding** command

| Parameter         | Description                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------|
| Client IP Address | The IP address of the DHCP client.                                                                         |
| MAC Address       | The MAC address of the DHCP client.                                                                        |
| VLAN              | The VLAN ID the packet is received on.                                                                     |
| Port              | The Layer 2 port name the packet is received on.                                                           |
| Expires (sec)     | Always infinite for static bindings, or when the leave time in the DHCP message was 0xffffffff (infinite). |
| Type              | DHCP Snooping binding type: Static                                                                         |

**Related Commands** [ip source binding](#)  
[show ip dhcp snooping binding](#)

# 34

# RRP Snooping Commands

## Introduction

**Overview** This section provides an alphabetical reference for commands used to configure the Router Redundancy Protocol (RRP).

- Command List**
- “[ip rrp snooping](#)” on page 1104
  - “[show ip rrp snooping](#)” on page 1105

# ip rrp snooping

**Overview** Use this command to enable RRP snooping.  
Use the **no** variant of this command to disable RRP Snooping.

**Syntax** ip rrp snooping  
no ip rrp snooping

**Default** The default is **disabled**.

**Mode** Global Configuration

**Usage** Use this command to enable the RRP Snooping feature. You cannot use RRP Snooping at the same time as the following features:

- STP, RSTP, or MSTP, except for edge ports. RSTP is enabled by default. To disable it, use the command [spanning-tree enable](#) on page 446.
- Port security (the command **switchport port-security**)
- Port authentication
- EPSR
- Port mirroring

**Examples** The example below shows you how to enable RRP Snooping.

```
awplus# configure terminal
awplus(config)# ip rrp snooping
```

**Related Commands** [show ip rrp snooping](#)



# show ip rrp snooping

**Overview** Use this command to display Router Redundancy Protocol snooping global settings and status.

**Syntax** show ip rrp snooping

**Mode** Privileged Exec

**Output** The following example show the output display for the **show ip rrp snooping** command

|                             |           |                     |          |
|-----------------------------|-----------|---------------------|----------|
| awplus#show ip rrp snooping |           |                     |          |
| Status : Enabled            |           |                     |          |
| Vlan                        | Master    | Virtual MAC Address | UpTime   |
| -----                       | -----     | -----               | -----    |
| vlan1                       | Port1.0.1 | 00e0.2b00.0085      | 00:00:39 |
| -----                       | -----     | -----               | -----    |

The following table shows the output display for the **show ip rrp snooping** command

| Parameter           | Description                                                                             |
|---------------------|-----------------------------------------------------------------------------------------|
| Status              | Displays if RRP Snooping is enabled or disabled                                         |
| Vlan                | Displays the VLAN ID                                                                    |
| Master              | Displays the port ID connected to the master router or the network of the master router |
| Virtual MAC Address | Displays the virtual MAC address of the router                                          |
| UpTime              | Displays the time that the current master router has been the master router             |

**Related Commands** [ip rrp snooping](#)

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure EPSR. For more information, see the [EPSR Feature Overview and Configuration Guide](#).

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](#).

- Command List**
- “[debug epsr](#)” on page 1108
  - “[epsr](#)” on page 1109
  - “[epsr configuration](#)” on page 1110
  - “[epsr datavlan](#)” on page 1111
  - “[epsr enhancedrecovery enable](#)” on page 1112
  - “[epsr mode master controlvlan primary port](#)” on page 1113
  - “[epsr mode transit controlvlan](#)” on page 1114
  - “[epsr priority](#)” on page 1115
  - “[epsr state](#)” on page 1116
  - “[epsr trap](#)” on page 1117
  - “[show debugging epsr](#)” on page 1118
  - “[show epsr](#)” on page 1119
  - “[show epsr common segments](#)” on page 1125
  - “[show epsr config-check](#)” on page 1126
  - “[show epsr <epsr-instance>](#)” on page 1128
  - “[show epsr <epsr-instance> counters](#)” on page 1129
  - “[show epsr counters](#)” on page 1130

- [“show epsr summary”](#) on page 1131
- [“undebbug epsr”](#) on page 1132

# debug epsr

**Overview** This command enables EPSR debugging.  
The **no** variant of this command disables EPSR debugging.

**Syntax** debug epsr {info|msg|pkt|state|timer|all}  
no debug epsr {info|msg|pkt|state|timer|all}

| Parameter | Description                                                                                                                                                                                                              |
|-----------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| info      | Send general EPSR information to the console.<br>Using this parameter with the <b>no debug epsr</b> command will explicitly exclude the above information from being sent to the console.                                |
| msg       | Send the decoded received and transmitted EPSR packets to the console.<br>Using this parameter with the <b>no debug epsr</b> command will explicitly exclude the above packets from being sent to the console.           |
| pkt       | Send the received and transmitted EPSR packets as raw ASCII text to the console.<br>Using this parameter with the <b>no debug epsr</b> command will explicitly exclude the above packets from being sent to the console. |
| state     | Send EPSR state transitions to the console.<br>Using this parameter with the <b>no debug epsr</b> command will explicitly exclude state transitions from being sent to the console.                                      |
| timer     | Send EPSR timer information to the console.<br>Using this parameter with the <b>no debug epsr</b> command will explicitly exclude timer information from being sent to the console.                                      |
| all       | Send all EPSR debugging information to the console.<br>Using this parameter with the <b>no debug epsr</b> command will explicitly exclude any debugging information from being sent to the console.                      |

**Mode** Privileged Exec and Global Configuration

**Examples** To enable state transition debugging, use the command:

```
awplus# debug epsr state
```

To disable EPSR packet debugging, use the command:

```
awplus# no debug epsr pkt
```

**Related Commands** [undebg epsr](#)

## epsr

**Overview** This command sets the timer values for an EPSR instance. These are only valid for master nodes.

**Syntax** `epsr <epsr-instance> {hellotime <1-32767>|failovertime <2-65535> ringflaptime <0-65535>}`  
`no epsr <epsr-instance>`

**CAUTION:** Using the “no” variant of this command will remove the specified EPSR instance.

| Parameter                                 | Description                                                                                                                                                                                                                                                                                                                          |
|-------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;epsr-instance&gt;</code>        | Name of the EPSR instance.                                                                                                                                                                                                                                                                                                           |
| <code>hellotime &lt;1-32767&gt;</code>    | The number of seconds between the transmission of health check messages.                                                                                                                                                                                                                                                             |
| <code>failovertime &lt;2-65535&gt;</code> | The number of seconds that a master waits for a returning health check message before entering the failed state. <b>The failover time should be greater than twice the hellotime.</b> This is to force the master node to wait until it detects the absence of two sequential healthcheck messages before entering the failed state. |
| <code>ringflaptime &lt;0-65535&gt;</code> | The minimum number of seconds that a master must remain in the failed state.                                                                                                                                                                                                                                                         |

**Mode** EPSR Configuration

**Examples** To set the hellotimer to 5 seconds for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue hellotime 5
```

To delete the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue
```

# epsr configuration

**Overview** Use this command to enter EPSR Configuration mode so that EPSR can be configured.

**Syntax** `epsr configuration`

**Mode** Global Configuration

**Example** To change to EPSR mode, use the command:

```
awplus(config)# epsr configuration
```

**Related Commands** [epsr mode master control](#)[vlan primary port](#)  
[epsr](#)  
[show epsr](#)

# epsr datavlan

**Overview** This command adds a data VLAN or a range of VLAN identifiers to a specified EPSR instance.

The **no** variant of this command removes a data VLAN or data VLAN range from an EPSR instance.

**Syntax** `epsr <epsr-instance> datavlan {<vlanid>|<vlanid-range>}`  
`no epsr <epsr-instance> datavlan {<vlanid>|<vlanid-range>}`

| Parameter       | Description                                                                                      |
|-----------------|--------------------------------------------------------------------------------------------------|
| <epsr-instance> | Name of the EPSR instance.                                                                       |
| datavlan        | Adds a data VLAN to be protected by the EPSR instance.                                           |
| <vlanid>        | The VLAN's VID - a number between 1 and 4094 excluding the number selected for the control VLAN. |
| <vlanid-range>  | Specify a range of VLAN identifiers using a hyphen to separate identifiers.                      |

**Mode** EPSR Configuration

**Usage** We recommend you

- set the EPSR control VLAN to `vlan2`, using the [epsr mode master controlvlan primary port](#) and [epsr mode transit controlvlan](#) commands, then
- set the EPSR data VLAN between to be a value between 3 and 4094, using the [epsr datavlan](#) command.

**Examples** To add `vlan3` to the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue datavlan vlan3
```

To add `vlan2` and `vlan3` to the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue datavlan vlan2-vlan3
```

To remove `vlan3` from the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue datavlan vlan3
```

To remove `vlan2` and `vlan3` from the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue datavlan vlan2-vlan3
```

**Related Commands** [epsr mode master controlvlan primary port](#)  
[epsr mode transit controlvlan](#)  
[show epsr](#)

# epsr enhancedrecovery enable

**Overview** This command enables EPSR's enhanced recovery mode. Enhanced recovery mode enables a ring to apply additional recovery procedures when a ring with more than one break partially mends. For more information, see the [EPSR Feature Overview and Configuration Guide](#).

The **no** variant of this command disables the enhanced recovery mode.

**Syntax** `epsr <epsr-instance> enhancedrecovery enable`  
`no epsr <epsr-instance> enhancedrecovery enable`

| Parameter                          | Description                |
|------------------------------------|----------------------------|
| <code>&lt;epsr-instance&gt;</code> | Name of the EPSR instance. |

**Default** Default is that enhanced recovery mode disabled.

**Mode** EPSR Configuration

**Example** To apply enhanced recovery on the EPSR instance called `blue`, use the command:  
`awplus(config-epsr)# epsr blue enhancedrecovery enable`

**Related Commands** [show epsr](#)



# epsr mode master controlvlan primary port

**Overview** This command creates a master EPSR instance.

**Syntax** `epsr <epsr-instance> mode master controlvlan <2-4094>  
primaryport <port>`

| Parameter       | Description                                                                                                                                         |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <epsr-instance> | Name of the EPSR instance.                                                                                                                          |
| mode            | Determines the node is acting as a master.                                                                                                          |
| master          | Sets switch to be the master node for the named EPSR ring.                                                                                          |
| controlvlan     | The VLAN that will transmit EPSR control frames.                                                                                                    |
| <2-4094>        | VLAN id.                                                                                                                                            |
| primaryport     | Primary port for the EPSR instance.                                                                                                                 |
| <port>          | The primary port. The port may be a switch port (e.g. port1.0.4) or a static channel group (e.g. sa2). It cannot be a dynamic (LACP) channel group. |

**NOTE:** The software allows you to configure more than two ports or static channel groups to the control VLAN within a single switch. However, we advise against this because in certain situations it can produce unpredictable results.

**Mode** EPSR Configuration

**Example** To create a master EPSR instance called blue with vlan2 as the control VLAN and port1.0.1 as the primary port, use the command:

```
awplus(config-epsr)# epsr blue mode master controlvlan vlan2
primaryport port1.0.1
```

**Related Commands** [epsr mode transit controlvlan](#)  
[show epsr](#)

# epsr mode transit controlvlan

**Overview** This command creates a transit EPSR instance.

**Syntax** `epsr <epsr-instance> mode transit controlvlan <2-4094>`

| Parameter       | Description                                                 |
|-----------------|-------------------------------------------------------------|
| <epsr-instance> | Name of the EPSR instance.                                  |
| mode            | Determines the node is acting as a transit node.            |
| transit         | Sets switch to be the transit node for the named EPSR ring. |
| controlvlan     | The VLAN that will transmit EPSR control frames.            |
| <2-4094>        | VLAN id.                                                    |

**NOTE:** The software allows you to configure more than two ports or static channel groups to the control VLAN within a single switch. However, we advise against this because in certain situations it can produce unpredictable results.

If the control VLAN contains more than two ports (or static channels) an algorithm selects the two ports or channels with the lowest number to be the ring ports. However if the switch has only one channel group is defined to the control vlan, EPSR will not operate on the secondary port.

EPSR does not support Dynamic link aggregation (LACP).

**Mode** EPSR Configuration

**Example** To create a transit EPSR instance called blue with vlan2 as the control VLAN, use the command:

```
awplus(config-epsr)# epsr blue mode transit controlvlan vlan2
```

**Related Commands**

- [epsr mode master controlvlan primary port](#)
- [epsr mode transit controlvlan](#)
- [show epsr](#)

## epsr priority

**Overview** This command sets the priority of an EPSR instance on an EPSR node. Priority is used to prevent “superloops” forming under fault conditions with particular ring configurations. Setting a node to have a priority greater than one, also has the effect of turning on **superloop protection**.

The **no** variant of this command returns the priority of the EPSR instance back to its default value of 0, which also disables EPSR Superloop prevention.

**Syntax** `epsr <epsr-instance> priority <0-127>`  
`no <epsr-instance> priority`

| Parameter       | Description                                                                                   |
|-----------------|-----------------------------------------------------------------------------------------------|
| <epsr-instance> | Name of the EPSR instance.                                                                    |
| priority        | The priority of the ring instance selected by the epsr-name parameter.                        |
| <0-127>         | The priority to be applied (0 is the lowest priority and represents no superloop protection). |

**Default** The default priority of an EPSR instance on an EPSR node is 0. The negated form of this command resets the priority of an EPSR instance on an EPSR node to the default value.

**Mode** EPSR Configuration

**Example** To set the priority of the EPSR instance called `blue` to the highest priority (127), use the command:

```
awplus(config-epsr)# epsr blue priority 127
```

To reset the priority of the EPSR instance called `blue` to the default (0), use the command:

```
awplus(config-epsr)# no epsr blue priority
```

**Related Commands** [epsr configuration](#)

## epsr state

**Overview** This command enables or disables an EPSR instance.

**Syntax** `epsr <epsr-instance> state {enabled|disabled}`

| Parameter                          | Description                        |
|------------------------------------|------------------------------------|
| <code>&lt;epsr-instance&gt;</code> | The name of the EPSR instance.     |
| <code>state</code>                 | The operational state of the ring. |
| <code>enabled</code>               | EPSR instance is enabled.          |
| <code>disabled</code>              | EPSR instance is disabled.         |

**Mode** EPSR Configuration

**Example** To enable the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue state enabled
```

**Related Commands** [epsr mode master controlvlan primary port](#)  
[epsr mode transit controlvlan](#)

## epsr trap

**Overview** This command enables SNMP traps for an EPSR instance. The traps will be sent when the EPSR instance changes state.

The **no** variant of this command disables SNMP traps for an EPSR instance. The traps will no longer be sent when the EPSR instance changes state.

**Syntax** `epsr <epsr-instance> trap`  
`no epsr <epsr-instance> trap`

| Parameter                          | Description                      |
|------------------------------------|----------------------------------|
| <code>&lt;epsr-instance&gt;</code> | Name of the EPSR instance.       |
| <code>trap</code>                  | SNMP trap for the EPSR instance. |

**Mode** EPSR Configuration

**Example** To enable traps for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue trap
```

To disable traps for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue trap
```

**Related Commands** [epsr mode master controlvlan primary port](#)  
[epsr mode transit controlvlan](#)  
[show epsr](#)

# show debugging epsr

**Overview** This command shows the debugging modes enabled for EPSR.

**Syntax** show debugging epsr

**Mode** User Exec and Privileged Exec

**Example** To show the enabled debugging modes, use the command:

```
awplus# show debugging epsr
```

**Related  
Commands** [debug epsr](#)

# show epsr

**Overview** This command displays information about all EPSR instances.

**Syntax** show epsr

**Mode** User Exec and Privileged Exec

**Example** To show the current settings of all EPSR instances, use the command:

```
awplus# show epsr
```

**Output:**  
**non-superloop**  
**topology**

The following examples show the output display for a non-superloop topology network.

Table 35-1: Example output from the **show epsr** command run on a transit node

| EPSR Information            |            |
|-----------------------------|------------|
| Name .....                  | test2      |
| Mode .....                  | Transit    |
| Status .....                | Enabled    |
| State .....                 | Links-Up   |
| Control Vlan .....          | 2          |
| Data VLAN(s) .....          | 10         |
| Interface Mode .....        | Ports Only |
| First Port .....            | port1.0.1  |
| First Port Status .....     | Down       |
| First Port Direction .....  | Unknown    |
| Second Port .....           | port1.0.2  |
| Second Port Status .....    | Down       |
| Second Port Direction ..... | Unknown    |
| Trap .....                  | Enabled    |
| Master Node .....           | Unknown    |
| Enhanced Recovery .....     | Disabled   |

Table 35-2: Example output from the **show epsr** command run on a master node

| EPSR Information            |            |
|-----------------------------|------------|
| Name .....                  | test4      |
| Mode .....                  | Master     |
| Status .....                | Enabled    |
| State .....                 | Complete   |
| Control Vlan .....          | 4          |
| Data VLAN(s) .....          | 20         |
| Interface Mode .....        | Ports Only |
| Primary Port .....          | port1.0.3  |
| Primary Port Status .....   | Forwarding |
| Secondary Port .....        | port1.0.4  |
| Secondary Port Status ..... | Forwarding |
| Hello Time .....            | 1 s        |
| Failover Time .....         | 2 s        |
| Ring Flap Time .....        | 0 s        |
| Trap .....                  | Enabled    |
| Enhanced Recovery .....     | Disabled   |

**NOTE:** The above screen is only viewable when running the switch as an EPSR Master.



**Output:** The following examples show the output display for superloop topology network.  
**superloop**  
**topology**

Table 35-3: Example output from the **show epsr** command run on a Master Node

| EPSR Information           |                                 |
|----------------------------|---------------------------------|
| -----                      |                                 |
| Name .....                 | test4                           |
| Mode .....                 | Master                          |
| Status .....               | Enabled                         |
| State .....                | Complete                        |
| Control Vlan .....         | 4                               |
| Data VLAN(s) .....         | 20                              |
| Interface Mode .....       | Ports Only                      |
| Primary Port .....         | port1.0.3                       |
| Status .....               | Forwarding (logically blocking) |
| Is On Common Segment ..... | No                              |
| Blocking Control .....     | Physical                        |
| Secondary Port .....       | port1.0.4                       |
| Status .....               | Blocked                         |
| Is On Common Segment ..... | No                              |
| Blocking Control .....     | Physical                        |
| Hello Time .....           | 1 s                             |
| Failover Time .....        | 2 s                             |
| Ring Flap Time .....       | 0 s                             |
| Trap .....                 | Enabled                         |
| Enhanced Recovery .....    | Disabled                        |
| SLP Priority .....         | 12                              |
| -----                      |                                 |

**NOTE:** The above screen is only viewable when running the switch as an EPSR Master.

Table 35-4: Example output from the **show epsr** command run on a Transit Node

```

EPSR Information

Name test4
Mode Transit
Status Enabled
State Complete
Control Vlan 4
Data VLAN(s) 20
Interface Mode Ports Only
Primary Port port1.0.3
 Status Forwarding (logically blocking)
 Is On Common Segment No
 Blocking Control Physical
Secondary Port port1.0.4
 Status Blocked
 Is On Common Segment No
 Blocking Control Physical
Hello Time 1 s
Failover Time 2 s
Ring Flap Time 0 s
Trap Enabled
Enhanced Recovery Disabled
SLP Priority 12

```

Table 35-5: Parameters displayed in the output of the **show epsr** command

| Parameter on Master Node | Parameter on Transit Node | Description                                                                                                                                                       |
|--------------------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                     | Name                      | The name of the EPSR instance.                                                                                                                                    |
| Mode                     | Mode                      | The mode in which the EPSR instance is configured - either Master or Transit                                                                                      |
| Status                   | Status                    | Indicates whether the EPSR instance is enabled or disabled                                                                                                        |
| State                    | State                     | Indicates state of the EPSR instance's state machine. Master states are: Idle, Complete, and Failed. Transit states are Links-Up, Links-Down, and Pre-Forwarding. |
| Control Vlan             | Control Vlan              | Displays the VID of the EPSR instance's control VLAN.                                                                                                             |
| Data VLAN(s)             | Data VLAN(s)              | The VID(s) of the instance's data VLANs.                                                                                                                          |
| Interface Mode           | Interface Mode            | Whether the EPSR instance's ring ports are both physical ports (Ports Only) or are both static aggregators (Channel Groups Only).                                 |
| Primary Port             | First Port                | The EPSR instance's primary ring port.                                                                                                                            |

Table 35-5: Parameters displayed in the output of the **show epsr** command (cont.)

| Parameter on Master Node | Parameter on Transit Node | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| - Status                 | - Status                  | Whether the ring port is forwarding (Forwarding) or blocking (Blocked), or has link down (Down), and if forwarding or blocking, "(logical)" indicates the instance has only logically set the blocking state of the port because it does not have physical control of it.                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                          | - Direction               | The ring port on which the last EPSR control packet was received is indicated by "Upstream". The other ring port is then "Downstream"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| - Is On Common Segment   | - Is On Common Segment    | Whether the ring port is on a shared common segment link to another node, and if so, "(highest rank)" indicates it is the highest priority instance on that common segment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| - Blocking Control       | - Blocking Control        | Whether the instance has "physical" or "logical" control of the ring port's blocking in the instance's data VLANs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Secondary Port           | Second Port               | The EPSR instance's secondary port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| - Status                 | - Status                  | Whether the ring port is forwarding (Forwarding) or blocking (Blocked), or has link down (Down), and if forwarding or blocking, "(logical)" indicates the instance has only logically set the blocking state of the port, because it does not have physical control of it. Note that on a master configured for SuperLoop Prevention (non-zero priority) its secondary ring port can be physically forwarding, but logically blocking. This situation arises when it is not the highest priority node in the topology (and so does not receive LINKS-DOWN messages upon common segment breaks) and a break on a common segment in its ring is preventing reception of its own health messages. |
|                          | - Direction               | The ring port on which the last EPSR control packet was received is indicated by "Upstream". The other ring port is then "Downstream"                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| - Is On Common Segment   | - Is On Common Segment    | Whether the ring port is on a shared common segment link to another node, and if so, "(highest rank)" indicates it is the highest priority instance on that common segment                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| - Blocking Control       | - Blocking Control        | Whether the instance has "physical" or "logical" control of the ring port's blocking in the instance's data VLANs                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Hello Time               |                           | The EPSR instance's setting for the interval between transmissions of health check messages (in seconds)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Failover Time            |                           | The time (in seconds) the EPSR instance waits to receive a health check message before it decides the ring is down                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Ring Flap Time           |                           | The minimum time the EPSR instance must remain in the failed state                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Trap                     | Trap                      | Whether the EPSR instance has EPSR SNMP traps enabled                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

Table 35-5: Parameters displayed in the output of the **show epsr** command (cont.)

| Parameter on Master Node | Parameter on Transit Node | Description                                                  |
|--------------------------|---------------------------|--------------------------------------------------------------|
| Enhanced Recovery        | Enhanced Recovery         | Whether the EPSR instance has enhanced recovery mode enabled |
| SLP Priority             | SLP Priority              | The EPSR instance's priority (for SuperLoop Prevention)      |

**Related Commands**

- [epsr mode master controlvlan primary port](#)
- [epsr mode transit controlvlan](#)
- [show epsr counters](#)

# show epsr common segments

**Overview** This command displays information about all the superloop common segment ports on the switch.

**Syntax** show epsr common segments

**Example** To display information about all the superloop common segment ports on the switch, use the command:

```
awplus# show epsr common segments
```

Table 35-6: Example output from the **show epsr common segments** command

| EPSR Common Segments    |                  |         |      |              |                       |                     |
|-------------------------|------------------|---------|------|--------------|-----------------------|---------------------|
| Common Seg<br>Ring Port | EPSR<br>Instance | Mode    | Prio | Port<br>Type | Phys Ctrl<br>of Port? | Ring<br>Port Status |
| port1.0.24              | test_inst_Red    | Transit | 127  | Second       | Yes                   | Fwding              |
|                         | test_inst_Blue   | Transit | 126  | Second       | No                    | Fwding (logical)    |
|                         | test_inst_Green  | Transit | 125  | First        | No                    | Fwding (logical)    |
| sa4                     | testA            | Master  | 15   | Primary      | Yes                   | Blocking            |
|                         | testB            | Transit | 14   | Second       | No                    | Fwding (logical)    |
| sa5                     | test_55          | Transit | 8    | First        | Yes                   | Down                |
|                         | test_77          | Transit | 7    | First        | No                    | Down                |

**Related  
Commands** [show epsr](#)  
[show epsr summary](#)  
[show epsr counters](#)

# show epsr config-check

**Overview** This command checks the configuration of a specified EPSR instance, or all EPSR instances.

If an instance is enabled, this command will check for the following errors or warnings:

- The control VLAN has the wrong number of ports.
- There are no data VLANs.
- Some of the data VLANs are not assigned to the ring ports.
- The failover time is less than 5 seconds, for a stacked device.
- The instance is a master that shares a common segment with a higher priority instance.
- The instance is a master that shares a common segment with another master.
- The instance is a master with its secondary port on a common segment.

**Syntax** show epsr [*<instance>*] config-check

| Parameter               | Description                            |
|-------------------------|----------------------------------------|
| <i>&lt;instance&gt;</i> | Name of the EPSR instance to check on. |

**Mode** User Exec and Privileged Exec

**Example** To check the configuration of all EPSR instances and display the results, use the command:

```
awplus# show epsr config-check
```

Table 35-7: Example output from the **show epsr** config-check command

| EPSR Instance                                                                                        | Status  | Description                                                     |
|------------------------------------------------------------------------------------------------------|---------|-----------------------------------------------------------------|
| red                                                                                                  | Warning | Failover time is 2s but should be 5s because device is stacked. |
| white                                                                                                | OK.     |                                                                 |
| blue                                                                                                 | Warning | Primary port is not in data VLANs 29-99.                        |
| orange                                                                                               | OK.     |                                                                 |
| Don't forget to check that this node's configuration is consistent with all other nodes in the ring. |         |                                                                 |

**Related  
Commands** [show epsr](#)

# show epsr <epsr-instance>

**Overview** This command displays information about the specified EPSR instance.

**Syntax** show epsr <epsr-instance>

| Parameter       | Description                |
|-----------------|----------------------------|
| <epsr-instance> | Name of the EPSR instance. |

**Mode** User Exec and Privileged Exec

**Example** To show the current settings of the EPSR instance called blue, use the command:

```
awplus# show epsr blue
```

**Related Commands**

- [epsr mode master controlvlan primary port](#)
- [epsr mode transit controlvlan](#)
- [show epsr counters](#)



# show epsr <epsr-instance> counters

**Overview** This command displays counter information about the specified EPSR instance.

**Syntax** show epsr <epsr-instance> counters

| Parameter       | Description                |
|-----------------|----------------------------|
| <epsr-instance> | Name of the EPSR instance. |

**Mode** User Exec and Privileged Exec

**Example** To show the counters of the EPSR instance called blue, use the command:

```
awplus# show epsr blue counters
```

**Related Commands**

- epsr mode master controlvlan primary port
- epsr mode transit controlvlan
- show epsr

# show epsr counters

**Overview** This command displays counter information about all EPSR instances.

**Syntax** show epsr counters

**Mode** User Exec and Privileged Exec

**Example** To show the counters of all EPSR instances, use the command:

```
awplus# show epsr counters
```

**Related Commands**

- [epsr mode master controlvlan primary port](#)
- [epsr mode transit controlvlan](#)
- [show epsr](#)

# show epsr summary

**Overview** This command displays summary information about all EPSR instances on the switch

**Syntax** show epsr summary

**Mode** User Exec and Privileged Exec

**Example** To display EPSR summary information, use the command:

```
awplus# show epsr summary
```

Table 35-8: Example output from the **show epsr summary** command

| EPSR Summary Information                                                                      |      |          |            |           |      |                         |                           |
|-----------------------------------------------------------------------------------------------|------|----------|------------|-----------|------|-------------------------|---------------------------|
| Abbreviations:                                                                                |      |          |            |           |      |                         |                           |
| M = Master node                                                                               |      |          |            |           |      |                         |                           |
| T = Transit node                                                                              |      |          |            |           |      |                         |                           |
| C = is on a common segment with other instances                                               |      |          |            |           |      |                         |                           |
| P = instance on a common segment has physical control of the shared port's data VLAN blocking |      |          |            |           |      |                         |                           |
| LB = ring port is Logically Blocking - applicable to master only                              |      |          |            |           |      |                         |                           |
| EPSR Instance                                                                                 | Mode | Status   | State      | Ctrl VLAN | Prio | Primary/1st Port Status | Secondary/2nd Port Status |
| test-12345                                                                                    | T    | Enabled  | Links-Down | 6         | 127  | Blocking (C,P)          | Blocking (C,P)            |
| test1                                                                                         | M    | Enabled  | Complete   | 5         | 12   | Fwding                  | Fwding (LB)               |
| test2                                                                                         | T    | Enabled  | Pre-Fwding | 4         | 126  | Fwding (C)              | Blocking (C)              |
| localB                                                                                        | T    | Disabled | Idle       | 40        | 0    | Unknown                 | Unknown                   |
| localC                                                                                        | T    | Disabled | Idle       | 41        | 0    | Unknown                 | Unknown                   |

# undebbug epsr

**Overview** This command applies the functionality of the **no** variant of the [debug epsr](#) command.

# 36

# AMF Commands

## Introduction

This chapter provides an alphabetical reference for AMF commands.

### 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 178, 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 accordingly apply an appropriate hostname to each device in your AMF network.

### Command List

- [“atmf area”](#) on page 1136
- [“atmf area password”](#) on page 1137
- [“atmf backup”](#) on page 1139
- [“atmf backup area-masters delete”](#) on page 1140
- [“atmf backup area-masters enable”](#) on page 1141
- [“atmf backup area-masters now”](#) on page 1142
- [“atmf backup area-masters synchronize”](#) on page 1143
- [“atmf backup bandwidth”](#) on page 1144
- [“atmf backup delete”](#) on page 1145
- [“atmf backup enable”](#) on page 1146
- [“atmf backup now”](#) on page 1147
- [“atmf backup server”](#) on page 1149
- [“atmf backup stop”](#) on page 1151
- [“atmf backup synchronize”](#) on page 1152

- [“atmf cleanup”](#) on page 1153
- [“atmf controller”](#) on page 1154
- [“atmf distribute firmware”](#) on page 1155
- [“atmf domain vlan”](#) on page 1157
- [“atmf enable”](#) on page 1159
- [“atmf group \(membership\)”](#) on page 1160
- [“atmf log-verbose”](#) on page 1162
- [“atmf management subnet”](#) on page 1163
- [“atmf management vlan”](#) on page 1165
- [“atmf master”](#) on page 1166
- [“atmf network-name”](#) on page 1167
- [“atmf provision”](#) on page 1168
- [“atmf provision node clone”](#) on page 1169
- [“atmf provision node configure boot config”](#) on page 1171
- [“atmf provision node configure boot system”](#) on page 1173
- [“atmf provision node create”](#) on page 1175
- [“atmf provision node delete”](#) on page 1177
- [“atmf provision node license-cert”](#) on page 1179
- [“atmf provision node locate”](#) on page 1181
- [“atmf reboot-rolling”](#) on page 1182
- [“atmf recover”](#) on page 1186
- [“atmf recover led-off”](#) on page 1188
- [“atmf remote-login”](#) on page 1189
- [“atmf restricted-login”](#) on page 1190
- [“atmf select-area”](#) on page 1191
- [“atmf virtual-link”](#) on page 1192
- [“atmf working-set”](#) on page 1195
- [“clear atmf links statistics”](#) on page 1197
- [“debug atmf”](#) on page 1198
- [“debug atmf packet”](#) on page 1200
- [“erase factory-default”](#) on page 1203
- [“show atmf”](#) on page 1204
- [“show atmf area”](#) on page 1208
- [“show atmf area summary”](#) on page 1211
- [“show atmf area nodes”](#) on page 1212

- [“show atmf area nodes-detail”](#) on page 1214
- [“show atmf backup”](#) on page 1216
- [“show atmf backup area”](#) on page 1219
- [“show atmf detail”](#) on page 1221
- [“show atmf group”](#) on page 1223
- [“show atmf group members”](#) on page 1225
- [“show atmf links”](#) on page 1227
- [“show atmf links detail”](#) on page 1228
- [“show atmf links statistics”](#) on page 1236
- [“show atmf memory”](#) on page 1241
- [“show atmf nodes”](#) on page 1243
- [“show atmf provision nodes”](#) on page 1244
- [“show atmf tech”](#) on page 1245
- [“show atmf working-set”](#) on page 1248
- [“show debugging atmf”](#) on page 1249
- [“show debugging atmf packet”](#) on page 1250
- [“show running-config atmf”](#) on page 1251
- [“switchport atmf-arealink remote-area”](#) on page 1252
- [“switchport atmf-crosslink”](#) on page 1253
- [“switchport atmf-link”](#) on page 1255
- [“type atmf node”](#) on page 1256
- [“undebg atmf”](#) on page 1259

# 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 <1-126> [local]`  
`no atmf area <area-name>`

| Parameter   | Description                                                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <area-name> | The AMF area name. Up to 15 printable characters can be entered for the name. Names are case sensitive and must be unique within an AMF network. |
| <1-126>     | 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** This command enables you to divide your AMF network into areas. Each area is managed by at least one 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 remote-area](#)



# 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** 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 area

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 remote-area

# 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>}  
no atmf backup enable

| 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** Running this command only configures the schedule. To enable the schedule, you should then apply the command [atmf backup enable](#).

**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 a 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 a backup of a specified node in a specified area. This command is only valid on AMF controllers.

**Syntax** `atmf backup area-masters delete area <area-name> node <node-name>`

| Parameter   | Description                                                   |
|-------------|---------------------------------------------------------------|
| <area-name> | The area that contains the node whose backup will be deleted. |
| <node-name> | 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 area 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** 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.

**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 a 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 Wellington area, 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 synchronise 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.

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                                       |
|-----------|---------------------------------------------------|
| <0-1000>  | 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.

**Syntax** atmf backup delete *<node-name>*

| Parameter                | Description                                         |
|--------------------------|-----------------------------------------------------|
| <i>&lt;node-name&gt;</i> | 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** 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 1216 to check the amount of space available on your external storage device.

**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 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.

**Syntax** atmf backup now [<nodename>]

| Parameter                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <nodename><br>or<br><hostname> | The name of the AMF member to be backed up, as set by the command <a href="#">hostname</a> on page 178. 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 host_0016_76b1_7a5e. 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** 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 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** 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.

**Syntax** atmf backup stop

**Mode** Privileged Exec

**Usage** 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.

**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** [show atmf backup](#)  
[atmf backup enable](#)  
[show atmf](#)



# atmf cleanup

**Overview** This command erases all data from NVS and all data from Flash **excluding** the following:

- The current release file and its /flash/.release file
- The backup release file and /flash/.backup file
- v1 license files /flash/.configs/.swfeature.lic
- v2 license files /flash/.configs/.sw\_v2.lic

It then reboots to put the device in a clean state ready to be used as a replacement node on a provisioned port.

**Syntax** atmf cleanup

**Mode** Privileged Exec

**Usage** This command is an alias to the [erase factory-default](#) command.

**Example** To erase data, use the command:

```
Node_1# atmf cleanup
```

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

**Related Commands** [erase factory-default](#)

# 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.

The number of areas supported on a controller depends on the license installed on that controller.

**Syntax** atmf controller  
no atmf controller

**Mode** Global configuration

**Usage** A valid AMF license must be available before this command can be applied.

**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 [reboot](#) 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 sw\_team, use the following commands:

```
SW_Team1# atmf working-set group sw_team
```

## Output

```
=====
SW_Team1, SW_Team2, SW_Team3:
=====
Working set join
```

```
ATMF_NETWORK[3]# atmf distribute firmware card:*.rel
```

## Output

```
Retrieving data from SW_Team1
Retrieving data from SW_Team2
Retrieving data from SW_Team3

ATMF Firmware Upgrade:

Node Name New Release File Status

SW_Team1 x510-main-20140204-2.rel Release ready
SW_Team2 x610-main-20140204-2.rel Release ready
SW_Team3 x610-main-20140204-2.rel Release ready
Continue the rolling reboot ? (y/n):y
=====
Copying Release : x510-main-20140204-2.rel to SW_Team1
Updating Release : x510-main-20140204-2.rel information on SW_Team1
=====
Copying Release : x610-main-20140204-2.rel to SW_Team2
Updating Release : x610-main-20140204-2.rel information on SW_Team2
=====
Copying Release : x610-main-20140204-2.rel to SW_Team3
Updating Release : x610-main-20140204-2.rel information on SW_Team3
=====
New firmware will not take effect until nodes are rebooted.
=====

ATMF_NETWORK[3]#
```

**Related** [atmf working-set](#)  
**Commands**

## atmf domain vlan

**Overview** The AMF domain vlan is one of the internal VLANs that are used to communicate information about the state of the AMF network between nodes. AMF uses its internal VLANs (the management VLAN and the domain VLAN) to communicate its inter nodal network status information. These VLANs must be reserved for AMF and not used for other purposes.

When an AMF network is first created all its nodes are assigned a domain VLAN with a default (domain) VID of 4091. An important point conceptually is that although this VLAN then 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.

If you assign a VLAN ID to this VLAN (i.e. changing its value from the default of 4091) then you will need to do this separately on every device within the AMF network. The AMF domain subnet will then be applied to this new VID when all devices within the AMF network are next rebooted.

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                             |
|-----------|-----------------------------------------|
| <2-4090>  | The VLAN number in the range 2 to 4090. |

**Default** The default domain VLAN ID for the AMF is 4091.

**Mode** Global Configuration

**Usage** The VLANs involved in this process must be reserved for AMF and cannot be used for other purposes. This command enables you to change the domain VLAN to match your network's specific configuration.

**CAUTION:** *Setting this command, then rebooting the device, will only apply the AMF VLAN for the device being configured. The new domain VLAN will not become effective for the AMF network until all its member nodes have been updated, and all its member devices rebooted.*

As part of its automatic creation process, this VLAN will also be assigned an IP subnet address based on the value configured by the command [atmf management subnet](#) on page 1163. Refer to this command for more information.

**Examples** To change the AMF domain VLAN to 4000 use the following commands:

```
node-1# configure terminal
node-1(config)# atmf domain vlan 4000
```

To reset the AMF domain VLAN to its default of 4091, use the following commands:

```
node-1# configure terminal
node-1(config)# no atmf domain 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** 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, x610, 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. x610, 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                                                                              |
|--------------|------------------------------------------------------------------------------------------|
| <group-list> | A list of group names. These should be entered as a comma delimited list without spaces. |

**Mode** Global Configuration

**Usage** 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 log-verbose

**Overview** This command limits the number of log messages displayed on the console or permanently logged.

**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 of this command description.

AMF uses these internal IPv4 subnets when exchanging its inter nodal status packets. These subnet addresses must be reserved for AMF and should be used for no other purpose.

The new management subnet will not become effective until all members of the AMF network have been updated and all its units rebooted.

Use the **no** variant of this command to remove the assigned subnet VLANs.

**Syntax** atmf management subnet <a.b.0.0>  
no atmf management subnet

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                     |
|-----------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a.b.0.0> | 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** Typically a network administrator would use this command to change the default subnet address to match local network requirements.

As previously mentioned, 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](#).

**Examples** To change the AMF management subnet address on node node-1 to 172.25.0.0:

```
node-1# configure terminal
node-1(config)# atmf management subnet 172.25.0.0
```

To change the AMF management subnet address on node node-1 back to its default of 172.31.0.0:

```
node-1# configure terminal
node-1(config)# no atmf management subnet
```

# atmf management vlan

**Overview** The AMF management VLAN is created when the AMF network is first initiated and is assigned its default VID of 4092. This command enables you to change the VID from this default value.

The AMF management vlan is one of the internal VLANs that are used to communicate information about the state of the AMF network between nodes. AMF uses its internal VLANS (such as the management VLAN and the domain VLAN) to communicate its inter nodal network status information. These VLANs must be reserved for AMF and not used for other purposes.

If you assign a VLAN ID to this VLAN (i.e. change its value from the default of 4092) then you will need to do this separately on every device within the AMF. The AMF management subnet will then be applied to this new VID when all devices within the AMF network are next rebooted.

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                                   |
|-----------|-----------------------------------------------|
| <2-4090>  | The VID assigned tro the AMF management VLAN. |

**Default** VLAN ID default is 4092

**NOTE:** Although the value applied by default lies outside the user configurable range. You can use the “no” variant of this command to reset the VLAN to its default value.

**mode** Global Configuration

**Usage** You can use this command to change the management VLAN to meet your network’s requirements and standards, particularly in situations where the default address value is unacceptable.

**NOTE:** This VLAN will automatically be assigned an IP subnet address based on the value configured by the command *atmf management subnet*. Refer to this command description for further details.

**Examples** To change the AMF management VLAN to 4090 use the following commands:

```
VCF-1# configure terminal
```

```
VCF-1(config)# atmf management vlan 4090
```

To reset the AMF domain VLAN to its default of 4092, use the following commands:

```
VCF-1# configure terminal
```

```
VCF-1(config)# no atmf management vlan 4090
```

# 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 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 [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                                                                              |
|-----------|------------------------------------------------------------------------------------------|
| <name>    | The AMF network name. Up to 15 printable characters can be entered for the network-name. |

**Mode** Global Configuration

**Usage** 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. This command will not take effect until the particular node is rebooted.

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

**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                                                                         |
|------------|-------------------------------------------------------------------------------------|
| <nodename> | The name of the provisioned node that will appear on the AMF network in the future. |

**Default** No provision.

**Mode** Interface Configuration

**Usage** 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 command:

```
host1(config)# interface port1.0.1
host1(config-if)# atmf provision node1
```

**Related Commands** [switchport atmf-link](#)  
[switchport atmf-crosslink](#)  
[show atmf links](#)



# atmf provision node clone

**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 [atmf provision node create](#).

**Syntax** `atmf provision node <nodename> clone <source-nodename>`

| Parameter         | Description                                                                        |
|-------------------|------------------------------------------------------------------------------------|
| <nodename>        | The name that will be assigned to the clone when connected.                        |
| <source-nodename> | The name of the node whose configuration is to be copied for loading to the clone. |

**Mode** Privileged Exec

**Usage** This command is only available on master nodes in the AMF network. You must run either this command or [atmf provision node create](#) command, before you can use other **atmf provision node** commands using the specified node name. If a backup or provisioned node already exists for the specified node then you must delete it before using the **atmf provision node clone** command.

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 clone device2
```

Figure 36-1: Sample output from the **atmf provision node clone** command

```
device1#atmf provision node device3 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 36-2: 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 Jan 2014 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 01 Jan 2014 00:05:49 No Yes Good
device2 01 Jan 2014 00:05:44 Yes Yes Good
```

# atmf provision node configure boot config

**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.

Use the **no** variant of this command to set back to the default.

**Syntax** `atmf provision node <nodename> configure boot config [backup] [<file-path|URL>]`  
`atmf provision node [<nodename>] configure no boot config [backup]`

| Parameter       | Description                                         |
|-----------------|-----------------------------------------------------|
| <nodename>      | The name of the provisioned node.                   |
| <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** Privileged Exec

**Usage** 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 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 node node1 configure boot config
backup usb:/atmf/amf_net/nodes/node1/config/backup.cfg
```

To unset the boot configuration, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
config
```

To unset the backup boot configuration, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
config backup
```

**Related  
Commands**    [atmf provision node configure boot system](#)  
                  [show atmf provision nodes](#)

# atmf provision node configure boot system

**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 set back to the default.

This command can only be run on AMF master nodes.

**Syntax** `atmf provision node <nodename> configure boot system [backup]  
[<file-path|URL>]`  
`atmf provision node <nodename> configure no boot system [backup]`

| Parameter       | Description                                   |
|-----------------|-----------------------------------------------|
| <nodename>      | The name of the provisioned node.             |
| <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** Privileged Exec

**Usage** 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 `x610-5.4.4-1.rel` on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot system
x610-5.4.4-1.rel
```

To set the backup release file `x610-5.4.4-1.rel` as the backup to the main release file on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot system
backup card:/atmf/amf_net/nodes/node1/flash/x610-5.4.4-1.rel
```

To unset the boot release, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
system
```

To unset the backup boot release, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
system backup
```

**Related  
Commands**    [atmf provision node configure boot config](#)  
                  [show atmf provision nodes](#)

# atmf provision node create

**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 [atmf provision node clone](#).

This command can only run on AMF master nodes.

**Syntax** `atmf provision node <nodename> create`

| Parameter  | Description                                     |
|------------|-------------------------------------------------|
| <nodename> | The name of the node that is being provisioned. |

**Mode** Privileged Exec

**Usage** This command is only available on master nodes in the AMF network.

The [atmf provision node create](#) command (or [atmf provision node clone](#)) must be executed before you can use other **atmf provision node** commands with the specified node name. If a backup or provisioned node already exists for the specified node name then you must delete it before using this command.

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 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 36-3: 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 02 Jan 2014 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 01 Jan 2014 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 node clone](#)



# atmf provision node delete

**Overview** This command deletes files that have been created for loading onto a provisioned node. It can only be run on master nodes.

**Syntax** `atmf provision node <nodename> delete`

| Parameter  | Description                                     |
|------------|-------------------------------------------------|
| <nodename> | The name of the provisioned node to be deleted. |

**Mode** Privileged Exec

**Usage** 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 **atmf provision node 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](#) 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 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 36-4: 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 Jan 2014 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 01 Jan 2014 00:05:49 No Yes Good
device2 01 Jan 2014 00:05:44 Yes Yes Good
```

**Related commands**   [atmf provision node create](#)

# atmf provision node license-cert

**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** atmf provision node {<nodename>} license-cert <file-path|URL>  
no atmf provision node {<nodename>} license-cert

| Parameter       | Description                                                                   |
|-----------------|-------------------------------------------------------------------------------|
| <nodename>      | The name of the provisioned node.                                             |
| <file-path URL> | 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** Privileged Exec

**Usage** 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 tftp server for AMF provisioned node *device2*, use the command:

```
device1# atmf provision node device2 license-cert
tftp://192.168.1.1/cert1.txt
```

**Example 2** To apply the license certificate cert2.txt stored on AMF master's flash directory for AMF provisioned node *host2*, use the command:

```
device1# atmf provision node device2 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 36-5: 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-May-2014 & 23:25:44
Provision Path : card:/atmf/nodes

Boot configuration :
Current boot image : x510-1766_atmf_backup.rel (file exists)
Backup boot image : x510-main-20140113-2.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** [show atmf provision nodes](#)

# atmf provision node locate

**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.

**Syntax** atmf provision node <nodename> locate

| Parameter  | Description                       |
|------------|-----------------------------------|
| <nodename> | The name of the provisioned node. |

**Mode** Privileged Exec

**Usage** 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. Otherwise, an error message is shown when the command is run.

**NOTE:** We advise that after running this command, you return to a known working directory, typically flash.

**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 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 36-6: 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 node create](#)
- [atmf provision node clone](#)
- [pwd](#)

# 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 command enforces a node reboot even if a previous node does not rejoin the AMF network. In this situation the unsuitable node will time-out and the rolling reboot process stops. 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                                                                                                                                          |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| force     | 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. |
| <url>     | The path to the software upgrade file.                                                                                                               |

**Mode** Privileged Exec

**Usage** 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 `card:/5.4.3/x*-5.4.3-*.rel` will select from the folder `card:/5.4.3` the latest file that matches the selection `x` (wildcard) `-5.4.3-` (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 x610 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 x510 nodes in an AMF network, use the following command:

```
Bld2_Floor_1# atmf working-set group x510
```

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 x510

=====
SW_Team1, SW_Team2, SW_Team3:
=====

Working set join

ATMF_NETWORK[3]#atmf reboot-rolling
ATMF Rolling Reboot Nodes:

Node Name Timeout
 (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 releases, use the following command:

```
Node_1# atmf working-set group all
ATMF_NETWORK[9]# atmf reboot-rolling
card:/5.4.3/x*-5.4.3-*.rel
```



ATMF Rolling Reboot Nodes:

| Node Name                            | Timeout<br>(Minutes) | New Release File   | Status        |
|--------------------------------------|----------------------|--------------------|---------------|
| -----                                |                      |                    |               |
| SW_Team1                             | 8                    | x510-5.4.3-0.5.rel | Release Ready |
| SW_Team2                             | 10                   | x510-5.4.3-0.5.rel | Release Ready |
| SW_Team3                             | 8                    | ---                | Not Supported |
| HW_Team1                             | 6                    | ---                | Incompatible  |
| Bld1_Floor_2                         | 2                    | x610-5.4.3-0.5.rel | Release Ready |
| Bld1_Floor_1                         | 4                    | ---                | Incompatible  |
| Building_1                           | 2                    | ---                | Incompatible  |
| Building_2                           | 2                    | x908-5.4.3-0.5.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                                                                                                                                                                                                                              |
|------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <node-name>            | The name of the device whose configuration is to be recovered or replicated.                                                                                                                                                             |
| master<br><node-name>  | 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 <node-name> | 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** 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 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 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>     | User name.  |
| <nodename> | Node name.  |

**Mode** Privileged Exec (This command will only run at privilege level 15)

**Usage** 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 (i.e. device reboot) you will be returned to the originating node.

The software will not allow you to run multiple remote login sessions. You must exit an existing session before starting a new one.

**Example 1** To remotely login from node Node10 to Node20 use the following command:

```
Node10# atmf remote-login node20
```

**Example 2** In this example, user Whitney is a valid user of node5. She can remotely login from node5 to node3 by using the following commands:

```
node5# atmf remote-login user whitney node3
node3> enable
```

**NOTE:** In the above example the user name whitney is valid on both nodes.

Therefore, to prevent unauthorized access, user names should be unique across all nodes within the AMF network.

# atmf restricted-login

**Overview** This command restricts the use of the [atmf working-set](#) on page 1195 command on all AMF master nodes to privilege 15 users only. Once entered on any AMF master node, this command will propagate across the network.

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.

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.

In the presence of a **master** node, its default of “atmf restricted-login disabled” will permeate to all its member nodes. Similarly, any change in this command’s status that is made on a master node, will also permeate to all its member nodes

**Example** To enable restricted login, use the command  
Node\_20(config)# atmf restricted-login node20

**Validation Command** [show atmf](#)

## 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                                                   |
|-------------|---------------------------------------------------------------|
| <area-name> | Connect to the remote area-master of the area with this name. |
| local       | Return to managing the local controller area.                 |

**Mode** Privileged Exec

**Usage** 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 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.

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>]  
no atmf virtual-link id <1-4094>`

| Parameter                      | Description                                                                                                                                                                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>ip</code>                | The Internet Protocol (IP).                                                                                                                                                                                                                                       |
| <code>&lt;a.b.c.d&gt;</code>   | The IP address, of the local amf node (at its interface to the tunnel) entered in a.b.c.d format.                                                                                                                                                                 |
| <code>remote-id</code>         | 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. |
| <code>&lt;1-4094&gt;</code>    | The ID range 1-32.                                                                                                                                                                                                                                                |
| <code>remote-ip</code>         | The IP address of the remote node                                                                                                                                                                                                                                 |
| <code>&lt;a.b.c.d&gt;</code>   | The IP address, of the remote node (at its interface to the tunnel) entered in a.b.c.d format.                                                                                                                                                                    |
| <code>remote-area</code>       | The remote area connected to this area virtual link                                                                                                                                                                                                               |
| <code>&lt;area-name&gt;</code> | The name of the remote area connected to this virtual link.                                                                                                                                                                                                       |

**Mode** Global Configuration

**Usage** 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. 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.

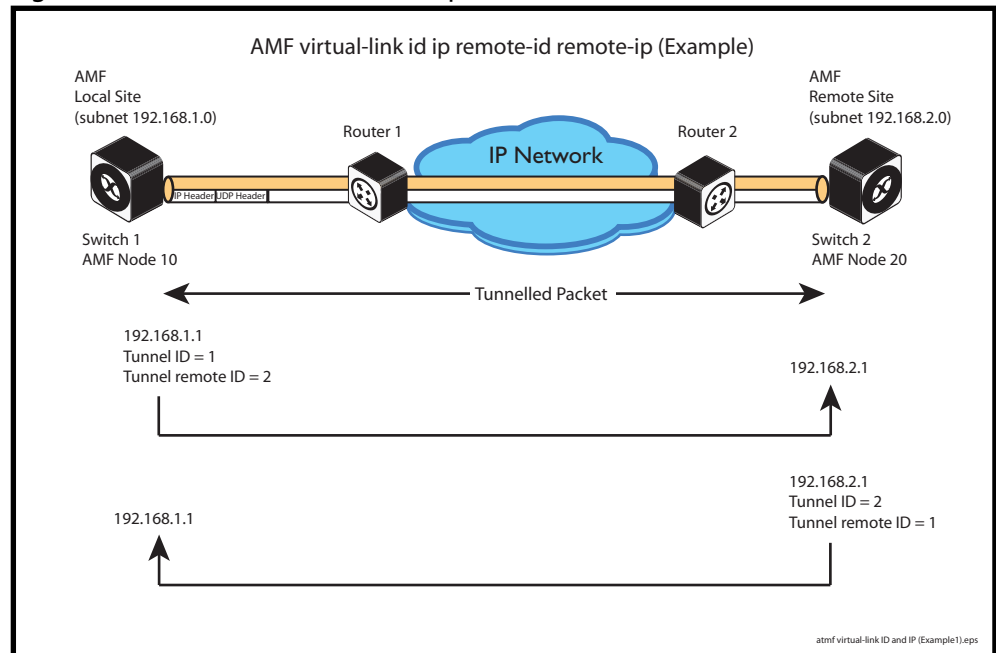


The tunneled link may operate via external (non AlliedWare Plus) routers in order to provide wide area network connectivity. However in this configuration, the routers perform a conventional router to router connection. The protocol tunneling function is accomplished by the AMF nodes.

**NOTE:** The requirement to pre-configure the local IP address and tunnel ID on a device located at the far end of an AMF virtual-link tunnel means that zero touch device replacement cannot be achieved on a remote device that terminates the tunnel connection.

**Example 1** Use the following commands to create the tunnel shown in the figure below.

Figure 36-7: 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*.

**Validation Command** `show atmf`

`show atmf links`

# atmf working-set

**Overview** The AMF working-set command enables you to execute commands across an individually listed set (or preselected group) of AMF nodes. Group selection is made 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 group output.

If a node is an AMF master it will be automatically added to the master group.

**Syntax** `atmf working-set`  
`{[<node-list>][group{<group-list>|all|local|current}]}`

| 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.                                                                                                                                                                                                           |

**Default** Needs to be entered

**Mode** Privileged Exec

**Example 1** To add all nodes in the AMF to the working-set, use the command:

```
node1# atmf 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 connectivity to only the local node; use the command:

```
ATMF_NETWORK_Name[6]# atmf working-set group local
node1#
```

| Parameter         | Description                                                                            |
|-------------------|----------------------------------------------------------------------------------------|
| node1, node2      | The name of the nodes - as set by the <a href="#">hostname</a> command.                |
| 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.                                                |

# 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](#)

# 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** 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 1259.

**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  
Commands** [no debug all](#)

# 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                                    |
|                          |  | [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 - [undebbug atmf](#) - can be found elsewhere in this chapter.

**Mode** User Exec and Global Configuration

**Usage** 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.                                           |



| Parameter  | Description                                                                                       |
|------------|---------------------------------------------------------------------------------------------------|
| timeout    | Sets the execution timeout for packet logging                                                     |
| <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 x610 interface port1.0.1 pkt-type 4 7 10
```

# erase factory-default

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

- The current release file and its /flash/.release file
- The backup release file and /flash/.backup file
- v1 license files /flash/.configs/.swfeature.lic
- v2 license files /flash/.configs/.sw\_v2.lic

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

**Syntax** erase factory-default

**Mode** Global Configuration.

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

**Example** To erase data, use the command:

```
Node_1(config)# erase factory-default
```

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

**Related Commands** [atmf cleanup](#)

# 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** 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 “Controlling “show” Command Output” in 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
```

The following figure shows some example output from running this command for a specific AMF node.

Table 36-1: 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                      | : Controller   |
| 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
```

The **show amf session** command displays all CLI (Command Line Interface) sessions for users that are currently logged in and running a CLI session. For example, in the case below, node\_1 and node5 have active users logged in.

**Example 3** To display AMF active sessions, use the following command:

```
node_1# show atmf session
```

Table 36-2: 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                            | : node5          |
| 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              |

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.

**Example 4** To display AMF technical information, use the following command:

```
node_1# show atmf tech
```

Table 36-3: 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 36-4: 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 36-4: 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 36-5: 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 36-6: 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 36-7: 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-area link remote-area</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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 36-7: Parameter definitions from the **show atmf area** command (cont.)

| Parameter       | Definition                                        |
|-----------------|---------------------------------------------------|
| 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 36-8: 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 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 36-9: 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 area nodes

**Overview** Use this command to display summarised information about an AMF controller's remote nodes.

**Syntax** show atmf area nodes [*<area-name>*] [*<node-name>*]

| Parameter                | Description                                             |
|--------------------------|---------------------------------------------------------|
| <i>&lt;area-name&gt;</i> | Displays information about nodes in the specified area. |
| <i>&lt;node-name&gt;</i> | Displays information about the specified node.          |

**Mode** Privileged Exec

**Usage** 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 summarised information about all the nodes the controller is aware of, use the command:

```
controller-1# show atmf area nodes
```

The following figure shows partial example output from running this command.

Table 36-10: Output from the **show atmf area nodes** command

|                                   |               |             |    |             |  |            |
|-----------------------------------|---------------|-------------|----|-------------|--|------------|
| controller-1#show atmf area nodes |               |             |    |             |  |            |
| Wellington Area Node Information: |               |             |    |             |  |            |
| Node Name                         | Device Type   | ATMF Master | SC | Parent      |  | Node Depth |
| -----                             |               |             |    |             |  |            |
| well-gate                         | x210-24GT     | N           | N  | well-master |  | 1          |
| well-master                       | AT-x930-28GPX | Y           | N  | none        |  | 0          |
| Wellington node count 2           |               |             |    |             |  |            |
| ...                               |               |             |    |             |  |            |

Table 36-11: 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.                |

Table 36-11: Parameter definitions from the **show atmf area nodes** command (cont.)

| Parameter   | Definition                                                                                            |
|-------------|-------------------------------------------------------------------------------------------------------|
| 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 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.

**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** 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 about all the nodes the controller is aware of, use the command:

```
controller-1# show atmf area nodes-detail
```

The following figure shows partial example output from running this command.

Table 36-12: Output from the **show atmf area nodes-detail** command

```

controller-1#show atmf area nodes-detail

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 36-13: 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        |                                                                                       |
| 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 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 [logs|server-status|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
```

```
Node_1# show atmf backup
ScheduledBackup Enabled
 Schedule.....1 per day starting at 03:00
 Next Backup Time....19 May 2012 03:00
Backup Media.....SD (Total 1974.0 MB, Free197.6MB)
Current Action.....Starting manual backup
Started.....18 May 2012 10:08
CurrentNode.....atmf_testbox1

Node Name Date Time In ATMF Status

atmf_testbox1 17May 2014 09:58:59 Yes Errors
atmf_testbox2 17May 2014 10:01:23 Yes Good

Node_1#show atmf backup logs

Log File Location: card:/atmf/office/logs/rsync_<nodename>.log

Node Name
 Log Details

atmf_testbox2
2014/05/22 03:41:32 [30299]File list size: 6199
2014/05/22 03:41:32 [30299]File list generation time: 0.011 seconds
2014/05/22 03:41:32 [30299]File list transfer time: 0.000 seconds
2014/05/22 03:41:32 [30299]Total bytes sent: 696
2014/05/22 03:41:32 [30299]Total bytes received: 16.03K
2014/02/20 03:41:32 [30299]sent 696 bytes received 16.03Kbytes 33.45 K bytes/sec
2014/05/22 03:41:32 [30299]total size is 21.73M speedup is 1298.93
2014/05/22 03:41:32 [30297]sent 626 bytes received 6203 bytes total size 43451648
```

**Example 2** 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 36-14: Parameter definitions from the **show atmf backup server-status** 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.               |

Table 36-14: Parameter definitions from the **show atmf backup server-status** command (cont.)

| Parameter         | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Backup Media      | The current backup medium in use. This will be one of USB, SD, or NONE. Note that the USB will take precedence over the SD card. 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.                                                                                                                                                                                                                                                                                                                                                          |
| Current Node      | The name of the node that is currently being backed up.                                                                                                                                                                                                                                                                                                                                                                                               |
| 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).                                                                                                                                                                                                                                                                                                                                                                                     |
| 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> </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 "Controlling "show" Command Output" in 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. This command is only available on AMF controllers.

**Syntax** `show atmf backup area [logs] [<area-name>] [<node-name>]`

| 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`

The following figure shows example output from running this command.

Table 36-15: 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 Apr 2015 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 -

```

| Area Name  | Node Name | Id | Date        | Time     | Status |
|------------|-----------|----|-------------|----------|--------|
| Wellington | camry     | 1  | 15 Apr 2015 | 02:30:22 | Good   |
| Canterbury | corona    | 1  | 15 Apr 2015 | 02:30:23 | Good   |
| Canterbury | Avensis   | 1  | 15 Apr 2015 | 02:30:22 | Good   |
| Auckland   | RAV4      | 1  | 15 Apr 2015 | 02:30:23 | Good   |
| Southland  | MR2       | 1  | 15 Apr 2015 | 02:30:24 | Good   |

**Related Commands**

- [atmf backup area-masters enable](#)
- [show atmf area](#)
- [show atmf area nodes-detail](#)
- [switchport atmf-arealink remote-area](#)

# 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:

|                               |                          |
|-------------------------------|--------------------------|
| controller-1#show atmf detail |                          |
| ATMF Detail Information:      |                          |
| Network Name                  | : Test_network           |
| Node Name                     | : controller-1           |
| Node Address                  | : controller-1.atmf      |
| Node ID                       | : 342                    |
| Node Depth                    | : 0                      |
| Domain State                  | : BackupDomainController |
| Recovery State                | : None                   |
| Log Verbose Setting           | : Verbose                |
| 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                   |

Table 36-16: Parameter definitions from the **show atmf detail** 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. |
| Node Name    | The name assigned to a particular node.            |

Table 36-16: Parameter definitions from the **show atmf detail** command (cont.)

| Parameter          | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. 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 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        | 'Y' if the node belongs to a Core domain.                                                                                                                                                                                                                                                                                                                                                                                                                |
| 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 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, x610. 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 1195. This can be seen from the network level prompt, which in this case is *AMF\_NETWORK[6]#*.

Table 36-17: 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 36-18: 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, x610, 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, x610. 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 36-19: 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 |
| x610                  | 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 36-20: 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 links

**Overview** This command displays brief information about AMF links on a device, such as link status and adjacent nodes.

Provisioned node names will be displayed with a trailing \* character, and will not have an entry under Adjacent Ifindex.

This command can only be run on AMF master and controller nodes.

**Syntax** show atmf links

**Mode** User Exec and Privileged Exec

**Example** To display the AMF links brief details, use the following command:

```
controller-1# show atmf links brief
```

Figure 36-8: Sample output from the **show atmf links** command

```
device1# show atmf link brief
```

| ATMF Links Brief: |           |             |            |               |                  |            |
|-------------------|-----------|-------------|------------|---------------|------------------|------------|
| Local Port        | Link Type | Port Status | ATMF State | Adjacent Node | Adjacent Ifindex | Link State |
| sa1               | Crosslink | Up          | TwoWay     | Building_1    | 4501             | Forwarding |
| 1.0.1             | Downlink  | Up          | Full       | Bld1_Floor_1  | 5001             | Forwarding |
| 1.0.2             | Downlink  | Up          | Full       | Bld1_Floor_2  | 5003             | Forwarding |
| 1.0.3             | Downlink  | Up          | Full       | Bld2_Floor_1  | 6101             | Forwarding |
| 1.0.4             | Crosslink | Down        | Init       | *device3      |                  | Blocking   |

\* = provisioned

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](#).

**Related Commands**

- [no debug all](#)
- [clear atmf links statistics](#)
- [show atmf](#)
- [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

**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.

Table 36-21: Sample output from the **show atmf links detail** command

|                                  |                     |
|----------------------------------|---------------------|
| device1# show atmf links details |                     |
| ATMF Links Detail:               |                     |
| Port                             | : sa1               |
| Ifindex                          | : 4501              |
| VR ID                            | : 0                 |
| Port Status                      | : Up                |
| Port State                       | : Full              |
| Port BPDU Receive Count          | : 44441             |
| Adjacent Node Name               | : Building_2        |
| Adjacent Ifindex                 | : 4501              |
| Adjacent VR ID                   | : 0                 |
| Adjacent MAC                     | : 0014.2299.137d    |
| Port Last Message Response       | : 0                 |
| Port                             | : port2.0.2         |
| Ifindex                          | : 6002              |
| VR ID                            | : 0                 |
| Port Status                      | : Down              |
| Port State                       | : Init              |
| Port BPDU Receive Count          | : 0                 |
| Link State Entries:              |                     |
| Node.Ifindex                     | : Building_2.4501 - |
| Building_1.4501                  |                     |
| Transaction ID                   | : 3 - 3             |
| MAC Address                      | : 0014.2299.137d -  |
| eccd.6d03.10e3                   |                     |
| Link State                       | : Full - Full       |
| Domain Nodes Tree:               |                     |
| Node                             | : Building_2        |
| Links on Node                    | : 1                 |
| Link 0                           | : Building_2.4501 - |
| Building_1.4501                  |                     |
| Forwarding State                 | : Forwarding        |
| Node                             | : Building_1        |
| Links on Node                    | : 1                 |
| Link 0                           | : Building_2.4501 - |
| Building_1.4501                  |                     |
| Forwarding State                 | : Forwarding        |
| Crosslink Transaction Entries:   |                     |
| Node                             | : Building_2        |
| Transaction ID                   | : 3                 |
| Uplink Transaction ID            | : 3                 |
| Uplink Information:              |                     |
| Waiting for Sync                 | : 0                 |
| Transaction ID                   | : 3                 |
| Number of Links                  | : 0                 |
| Number of Local Uplinks          | : 0                 |

Table 36-21: Sample output from the **show atmf links detail** command (cont.)

|                              |                         |
|------------------------------|-------------------------|
| Uplink Information:          |                         |
| Waiting for Sync             | : 0                     |
| Transaction ID               | : 3                     |
| Number of Links              | : 0                     |
| Number of Local Uplinks      | : 0                     |
| Originating Node             | : Building_2            |
| Domain                       | : -'s domain            |
| Node                         | : Building_2            |
| Ifindex                      | : 0                     |
| VR ID                        | : 0                     |
| Transaction ID               | : 3                     |
| Flags                        | : 32                    |
| Domain Controller            | : -                     |
| Domain Controller MAC        | : 0000.0000.0000        |
| Downlink Domain Information: |                         |
| Domain                       | : Bld2_Floor_1's domain |
| Domain Controller            | : Bld2_Floor_1          |
| Domain Controller MAC        | : eccd.6d3f.fef7        |
| Number of Links              | : 2                     |
| Number of Links Up           | : 2                     |
| Number of Links on This Node | : 1                     |
| Links are Blocked            | : 0                     |
| Node Transaction List        |                         |
| Node                         | : Building_2            |
| Transaction ID               | : 7                     |
| Domain List                  |                         |
| Domain                       | : Bld2_Floor_1's domain |
| Node                         | : Building_2            |
| Ifindex                      | : 5002                  |
| Transaction ID               | : 7                     |
| Flags                        | : 1                     |
| Domain                       | : Bld2_Floor_1's domain |
| Node                         | : Building_1            |
| Ifindex                      | : 7002                  |
| Transaction ID               | : 7                     |
| Flags                        | : 1                     |

Table 36-21: Sample output from the **show atmf links detail** command (cont.)

| Up/Downlink Ports Information  |                  |
|--------------------------------|------------------|
| Port                           | : port1.3.1      |
| Ifindex                        | : 7001           |
| VR ID                          | : 0              |
| Port Status                    | : Up             |
| Port State                     | : Full           |
| Adjacent Node                  | : Bld1_Floor_1   |
| Adjacent Internal ID           | : 4              |
| Adjacent Ifindex               | : 6001           |
| Adjacent Board ID              | : 290            |
| Adjacent VR ID                 | : 0              |
| Adjacent MAC                   | : 0000.cd37.0ea4 |
| Adjacent Domain Controller     | : Bld1_Floor_1   |
| Adjacent Domain Controller MAC | : 0000.cd37.0ea4 |
| Port Forwarding State          | : Blocking       |
| Port BPDU Receive Count        | : 0              |
| Port Sequence Number           | : 12             |
| Port Adjacent Sequence Number  | : 9              |
| Port Last Message Response     | : 0              |
| Port                           | : port1.3.2      |
| Ifindex                        | : 7002           |
| VR ID                          | : 0              |
| Port Status                    | : Up             |
| Port State                     | : Full           |
| Adjacent Node                  | : Bld2_Floor_1   |
| Adjacent Internal ID           | : 3              |
| Adjacent Ifindex               | : 5001           |
| Adjacent Board ID              | : 333            |
| Adjacent VR ID                 | : 0              |
| Adjacent MAC                   | : eccd.6d3f.fef7 |
| Adjacent Domain Controller     | : Bld2_Floor_1   |
| Adjacent Domain Controller MAC | : eccd.6d3f.fef7 |
| Port Forwarding State          | : Blocking       |
| Port BPDU Receive Count        | : 0              |
| Port Sequence Number           | : 15             |
| Port Adjacent Sequence Number  | : 8              |
| Port Last Message Response     | : 0              |

Table 36-22: Parameter definitions from the **show atmf links detail** command output

| Parameter        | Definition                                                       |
|------------------|------------------------------------------------------------------|
| Port Status      | Shows status of the local port on the Node as UP/DOWN.           |
| Adjacent Node    | Shows Adjacent AMF Node to this Node.                            |
| Adjacent IfIndex | Shows interface on the Adjacent AMF Node connected to this Node. |
| Link State       | Shows state of AMF link Forwarding/Blocking.                     |

Table 36-22: Parameter definitions from the **show atmf links detail** command output (cont.)

| 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 - Shows status of the local port on the Node as UP/DOWN.</li> <li>Port State - Same as AMF state as described above.</li> <li>Port BPDU Receive Count - The number of AMF protocol PDU's received.</li> <li>Adjacent Node Name - name of the adjacent node in the domain.</li> <li>Adjacent Ifindex - Ifindex of the adjacent node in the domain.</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>Show 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 36-22: 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 36-22: 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 “Controlling “show” Command Output” in 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 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 or a static channel 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 36-23: Sample output from the **show atmf links statistics** command

```
device1# show atmf links statistics
```

|                              |   |        |         |        |          |
|------------------------------|---|--------|---------|--------|----------|
| ATMF Statistics:             |   |        |         |        |          |
|                              |   |        | Receive |        | Transmit |
| -----                        |   |        |         |        |          |
| Arealink Hello               |   |        | 124082  |        | 124052   |
| Crosslink Hello              |   |        | 20665   |        | 20666    |
| Crosslink Hello Domain       |   |        | 10336   |        | 10338    |
| Crosslink Hello Uplink       |   |        | 10333   |        | 10338    |
| Hello Link                   |   |        | 41313   |        | 82649    |
| Hello Neighbor               |   |        | 0       |        | 0        |
| Hello Stack                  |   |        | 82652   |        | 82659    |
| Hello Gateway                |   |        | 165168  |        | 165281   |
| Database Description         |   |        | 42      |        | 43       |
| Database Request             |   |        | 16      |        | 3        |
| Database Update              |   |        | 2885    |        | 5496     |
| Database Update Bitmap       |   |        | 0       |        | 115      |
| Database Acknowledge         |   |        | 5331    |        | 2746     |
| Transmit Fails               |   |        | 0       |        | 38       |
| Discards                     |   |        | 4       |        | 0        |
| Total ATMF Packets           |   |        | 462823  |        | 504386   |
|                              |   |        |         |        |          |
| ATMF Database Statistics:    |   |        |         |        |          |
| Database Entries             |   |        | 15      |        |          |
| Database Full Ages           |   |        | 2       |        |          |
|                              |   |        |         |        |          |
| ATMF Packet Discards:        |   |        |         |        |          |
| Type0                        | 0 | Type1  | 0       | Type2  | 0        |
| Type3                        | 0 | Type4  | 0       | Type5  | 0        |
| Type6                        | 0 | Type7  | 0       | Type8  | 0        |
| Type9                        | 0 | Type10 | 0       | Type11 | 0        |
| Type12                       | 0 | Type13 | 0       | Type14 | 0        |
| Type15                       | 0 | Type16 | 0       | Type17 | 0        |
| Type18                       | 0 | Type19 | 0       | Type20 | 0        |
| Type21                       | 0 | Type22 | 0       |        |          |
|                              |   |        |         |        |          |
| ATMF Virtual Link Statistics |   |        |         |        |          |
| Virtual                      |   |        | Receive |        | Transmit |
| Link                         |   |        | Dropped |        | Dropped  |
| -----                        |   |        |         |        |          |
| vlink3                       |   |        | 97383   | 0      | 36260    |
|                              |   |        |         |        | 0        |

**Example 2** To display the AMF links statistics on interface port1.0.5, use the command:

```
device1# show atmf links statistics interface
port1.0.5
```

Figure 36-9: Sample output from the **show atmf links statistics** command for interface 1.0.5

```
device1# show atmf links statistics interface port1.0.5

ATMF Port Statistics:

Transmit Receive
port1.0.5 Crosslink Hello 231 232
port1.0.5 Crosslink Hello Domain 116 116
port1.0.5 Crosslink Hello Uplink 116 115
port1.0.5 Hello Link 0 0
```

Figure 36-10: 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. |

| Parameter            | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Database Full Ages   | Shows the number of times the entries aged in the database.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ATMF Packet Discards | <p>Shows the number of discarded packets of each type:</p> <ul style="list-style-type: none"> <li>• Type0: The number of discarded crosslink hello msgs received on a non crosslink port.</li> <li>• Type1: The number of discarded tx update packets - bad checksum.</li> <li>• Type2: The number of discarded tx update bitmap packets - bad checksum.</li> <li>• Type3: The number of discarded tx update packets - neighbor not in the correct state.</li> <li>• Type4: The number of discarded update packets - bad checksum.</li> <li>• Type5: The number of discarded update packets - neighbor not in the correct state.</li> <li>• Type6: The number of discarded update bitmap packets - bad checksum.</li> <li>• Type7: The number of discarded crosslink hello msgs received on a non crosslink port.</li> <li>• Type8: The number of discarded crosslink hello msg received on a port that is not in the correct state.</li> <li>• Type9: The number of discarded crosslink domain hello msgs received on a non crosslink port.</li> <li>• Type10: The number of discarded crosslink domain hello msgs received on a port that is not in the correct state.</li> <li>• Type11: The number of crosslink uplink hello msgs received on a non crosslink port.</li> <li>• Type12: The number of discarded crosslink uplink hello msgs ignored on a port that is not in the correct state.</li> <li>• Type13: The number of messages with an incorrect name for this AMF network.</li> <li>• Type14: The number of over-long packets received on a port.</li> <li>• Type15: The number of messages with a bad protocol version received on a port.</li> <li>• Type16: The number of messages with a bad packet checksum calculation received on a port.</li> <li>• Type17: The number of messages with a bad authentication type received on a port.</li> <li>• Type18: The number of messages with a bad simple password received on a port.</li> <li>• Type19: The number of discarded packets with an unsupported authentication type received on a port.</li> <li>• Type20: The number of discarded packets with an unknown neighbor received on a port.</li> </ul> |

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](#).

**Related  
Commands**    no debug all  
                 clear atmf links statistics  
                 show atmf



# show atmf memory

**Overview** This command displays a summary of the AMF memory usage. It can only be run on AMF master nodes.

**Syntax** show atmf memory

**Mode** User Exec

**Example** To display AMF memory allocations on Node\_1, use the command:

```
node_1# show atmf memory
```

Table 36-24: Sample output from the **show atmf memory** command

|                          |      |                 |    |        |               |
|--------------------------|------|-----------------|----|--------|---------------|
| node_1#show atmf memory  |      |                 |    |        |               |
| ATMF Memory Allocation:  |      |                 |    |        |               |
| Total memory allocated   |      | : 30020 (bytes) |    |        |               |
| Total memory allocations |      | : 77            |    |        |               |
| Line                     | 1238 | number          | 1  | memory | 28 (bytes)    |
| Line                     | 244  | number          | 2  | memory | 88 (bytes)    |
| Line                     | 3753 | number          | 2  | memory | 1872 (bytes)  |
| Line                     | 1616 | number          | 8  | memory | 320 (bytes)   |
| Line                     | 1391 | number          | 1  | memory | 60 (bytes)    |
| Line                     | 1837 | number          | 15 | memory | 600 (bytes)   |
| Line                     | 288  | number          | 1  | memory | 17716 (bytes) |
| Line                     | 3916 | number          | 1  | memory | 1520 (bytes)  |
| Line                     | 1623 | number          | 8  | memory | 320 (bytes)   |
| Line                     | 4477 | number          | 1  | memory | 1520 (bytes)  |
| Line                     | 659  | number          | 2  | memory | 512 (bytes)   |
| Line                     | 1844 | number          | 6  | memory | 600 (bytes)   |
| Line                     | 1749 | number          | 1  | memory | 32 (bytes)    |
| Line                     | 203  | number          | 6  | memory | 600 (bytes)   |
| Line                     | 4205 | number          | 1  | memory | 1520 (bytes)  |
| Line                     | 206  | number          | 4  | memory | 1524 (bytes)  |
| Line                     | 549  | number          | 1  | memory | 232 (bytes)   |
| Line                     | 3495 | number          | 1  | memory | 56 (bytes)    |
| Line                     | 2628 | number          | 2  | memory | 72 (bytes)    |
| Line                     | 678  | number          | 1  | memory | 32 (bytes)    |
| Line                     | 1423 | number          | 1  | memory | 48 (bytes)    |
| Line                     | 1733 | number          | 3  | memory | 492 (bytes)   |
| Line                     | 1611 | number          | 8  | memory | 256 (bytes)   |

Table 36-24: Sample output from the **show atmf memory** command (cont.)

|                            |      |        |              |        |              |
|----------------------------|------|--------|--------------|--------|--------------|
| ATMF Memory Deallocation:  |      |        |              |        |              |
| Total memory deallocated   |      | :      | 4958 (bytes) |        |              |
| Total memory deallocations |      | :      | 45           |        |              |
| Line                       | 1395 | number | 4            | memory | 400 (bytes)  |
| Line                       | 1956 | number | 1            | memory | 164 (bytes)  |
| Line                       | 1247 | number | 1            | memory | 52 (bytes)   |
| Line                       | 876  | number | 2            | memory | 80 (bytes)   |
| Line                       | 166  | number | 1            | memory | 232 (bytes)  |
| Line                       | 415  | number | 7            | memory | 587 (bytes)  |
| Line                       | 418  | number | 3            | memory | 300 (bytes)  |
| Line                       | 822  | number | 2            | memory | 80 (bytes)   |
| Line                       | 2341 | number | 4            | memory | 160 (bytes)  |
| Line                       | 3025 | number | 2            | memory | 88 (bytes)   |
| Line                       | 144  | number | 3            | memory | 1596 (bytes) |
| Line                       | 146  | number | 6            | memory | 312 (bytes)  |
| Line                       | 2349 | number | 4            | memory | 160 (bytes)  |
| Line                       | 1111 | number | 1            | memory | 59 (bytes)   |
| Line                       | 1393 | number | 4            | memory | 688 (bytes)  |
| -----                      |      |        |              |        |              |
| Total memory in use        |      | :      | 4958 (bytes) |        |              |
| Total memory items         |      | :      | 45           |        |              |

# show atmf nodes

**Overview** This command displays all nodes currently configured within the AMF network. It displays a topographical representation of the network infrastructure.

This command displays a summary of all virtual links currently in the running configuration.

**Syntax** show atmf nodes

**Mode** Privileged Exec

**Example** To display AMF information for all nodes in the AMF, use the command:

```
node_1# show atmf nodes
```

Table 36-25: Sample output from the **show atmf nodes** command.

```
node1#show atmf nodes
```

Node Information:

\* = Local device

SC = Switch Configuration:  
C = Chassis    S = Stackable    N = Standalone

| Node Name      | Device Type      | ATMF Master | SC | Parent       | Node Depth |
|----------------|------------------|-------------|----|--------------|------------|
| Building_1     | AT-SBx8112       | Y           | C  | -            | 0          |
| * Bld1_Floor_1 | SwitchBlade x908 | N           | S  | Building_1   | 1          |
| Bld1_Floor_2   | x600-24Ts/XP     | N           | N  | Building_1   | 1          |
| Bld2_Floor_1   | x610-24Ts-POE+   | N           | N  | Building_1   | 1          |
| SW_Team1       | x210-24GT        | N           | N  | Bld1_Floor_2 | 2          |

Current ATMF node count 6

# 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** 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 36-11: 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-May-2014 & 23:25:44
Provision Path : card:/atmf/provision_nodes

Boot configuration :
Current boot image : x510-1766_atmf_backup.rel (file exists)
Backup boot image : x510-main-20140113-2.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 node create](#)
- [atmf provision node clone](#)
- [atmf provision node configure boot config](#)
- [atmf provision node configure boot system](#)
- [show atmf backup](#)

# 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 36-26: 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
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 36-27: 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.        |

Table 36-27: Parameter definitions from the **show atmf tech** command (cont.)

| Parameter          | Definition                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 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) |
| 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 (= prefix /17)                   |
| Device Type        | Shows the Product Series Name.                                                                                                                                                                                                                                                                                                                                                                       |
| ATMF Master        | Indicates the nodes 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 to which connects 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 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 36-28: 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** This command shows the debugging modes status for AMF.

**Syntax** show debugging atmf

**Mode** User Exec and Global Configuration

**Example** To display the AMF debugging status, use the command:

```
node_1# show debugging atmf
```

Figure 36-12: Sample output from the **show debugging atmf** command.

```
node1# 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** This command shows details of AMF Packet debug command settings.

**Syntax** show debugging atmf packet

**Mode** User Exec and Global Configuration

**Example** To display the AMF packet debugging status, use the command:

```
node_1# show debug atmf packet
```

Figure 36-13: 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Related  
Commands** show running-config  
no debug all

# switchport atmf-arealink remote-area

**Overview** This command enables you to configure a port or aggregator to be an AMF arealink. AMF arealinks 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-arealink 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** By default, no arealinks are configured

**Mode** Interface Configuration

**Usage** 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.

**Example** To make a switchport 1.2.1 an arealink to the *Auckland* area on VLAN 6, use the following commands

```
controller-1# configure terminal
controller-1(config)# interface port1.2.1
controller-1(config-if)# switchport atmf-arealink remote-area
Auckland vlan 6
```

**Related Commands**

- [atmf area](#)
- [atmf area password](#)
- [atmf virtual-link](#)
- [show atmf links](#)

# switchport atmf-crosslink

**Overview** This command configures the selected port or (statically) aggregated link to be an AMF crosslink. Running this command will automatically place the port or static 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.

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

**Usage** 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** 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** 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** 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 atm links statistics](#)

# switchport atmf-link

- Overview** This command enables you to configure a port or aggregator to be an AMF uplink/downlink. Running this command will automatically place the port or aggregator into trunk mode.
- 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

## type atmf node

**Overview** This command configures a trigger to be activated at an AMF node join event or leave event.

**Syntax** type atmf node {join|leave}

| Parameter | Description           |
|-----------|-----------------------|
| join      | AMF node join event.  |
| leave     | AMF node leave event. |

**Mode** Trigger Configuration

**CAUTION:** *Only configure this trigger on one device because it is a network wide event.*

**Example 1** To configure trigger 5 to activate at an AMF node leave event, 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** [show trigger](#)  
**Commands**

# undebbug atmf

**Overview** This command is an alias for the **no** variant of the [debug atmf](#) command.

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure the Network Time Protocol (NTP). For more information, see the [NTP Feature Overview and Configuration Guide](#).

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](#).

- Command List**
- [“ntp access-group”](#) on page 1261
  - [“ntp authenticate”](#) on page 1262
  - [“ntp authentication-key”](#) on page 1263
  - [“ntp broadcastdelay”](#) on page 1264
  - [“ntp master”](#) on page 1265
  - [“ntp peer”](#) on page 1266
  - [“ntp server”](#) on page 1268
  - [“ntp source”](#) on page 1270
  - [“ntp trusted-key”](#) on page 1272
  - [“show counter ntp”](#) on page 1273
  - [“show ntp associations”](#) on page 1275
  - [“show ntp status”](#) on page 1277

## ntp access-group

**Overview** This command creates an NTP access group, and applies a basic IP access list to it. This allows you to control access to NTP services.

The **no** variant of this command removes the configured NTP access group.

**Syntax** `ntp access-group [peer | query-only | serve | serve-only]`  
`[<1-99> | <1300-1999>]`  
`no ntp access-group [peer | query-only | serve | serve-only]`

| Parameter   | Description                                                                                                                                                  |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|
| peer        | Allows time requests and NTP control queries, and allows the system to synchronize itself to a system whose address passes the access list criteria.         |
| query-only  | Allows only NTP control queries from a system whose address passes the access list criteria.                                                                 |
| serve       | Allows time requests and NTP control queries, but does not allow the system to synchronize itself to a system whose address passes the access list criteria. |
| serve-only  | Allows only time requests from a system whose address passes the access list criteria.                                                                       |
| <1-99>      | Standard IP access list.                                                                                                                                     |
| <1300-1999> | Expanded IP access list.                                                                                                                                     |

**Mode** Global Configuration

**Examples** To create an NTP peer access group for an extended IP access list, use the commands:

```
awplus# configure terminal
awplus(config)# ntp access-group peer 1998
```

To disable the NTP peer access group created above, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp access-group peer
```

# ntp authenticate

**Overview** This command enables NTP authentication. This allows NTP to authenticate the associations with other systems for security purposes.

The **no** variant of this command disables NTP authentication.

**Syntax** ntp authenticate  
no ntp authenticate

**Mode** Global Configuration

**Examples** To enable NTP authentication, use the commands:

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

To disable NTP authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp authenticate
```

# ntp authentication-key

**Overview** This command defines each of the authentication keys. Each key has a key number, a type, and a value. Currently, the only key type supported is MD5.

The **no** variant of this disables the authentication key assigned previously using **ntp authentication-key**.

**Syntax** ntp authentication-key <keynumber> md5 <key>  
no ntp authentication-key <keynumber> md5 <key>

| Parameter   | Description                    |
|-------------|--------------------------------|
| <keynumber> | <1-4294967295> The key number. |
| <key>       | The authentication key.        |

**Mode** Global Configuration

**Examples** To define an authentication key number 134343 and a key value mystring, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# ntp authentication-key 134343 md5 mystring
```

To disable the authentication key number 134343 with the key value mystring, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no ntp authentication-key 134343 md5 mystring
```

# ntp broadcastdelay

**Overview** Use this command to set the estimated round-trip delay for broadcast packets. Use the **no** variant of this command to reset the round-trip delay for broadcast packets to the default offset of 0 microseconds.

**Syntax** ntp broadcastdelay <delay>  
no ntp broadcastdelay

| Parameter | Description                                     |
|-----------|-------------------------------------------------|
| <delay>   | <1-999999> The broadcast delay in microseconds. |

**Default** 0 microsecond offset, which can only be applied with the **no** variant of this command.

**Mode** Global Configuration

**Examples** To set the estimated round-trip delay to 23464 microseconds for broadcast packets, use these commands:

```
awplus# configure terminal
awplus(config)# ntp broadcastdelay 23464
```

To reset the estimated round-trip delay for broadcast packets to the default setting (0 microseconds), use these commands:

```
awplus# configure terminal
awplus(config)# no ntp broadcastdelay
```



## ntp master

**Overview** Use this command to make the device to be an authoritative NTP server, even if the system is not synchronized to an outside time source. Note that no stratum number is set by default.

Use the **no** variant of this command to stop the device being the designated NTP server.

**Syntax** ntp master [<stratum>]  
no ntp master

| Parameter | Description                                                                                                  |
|-----------|--------------------------------------------------------------------------------------------------------------|
| <stratum> | <1-15> The stratum number defines the configured level that is set for this master within the NTP hierarchy. |

**Mode** Global Configuration

**Usage** The stratum number is null by default and must be set using this command. The stratum levels define the distance from the reference clock and exist to prevent cycles in the hierarchy. Stratum 1 is used to indicate time servers, which are more accurate than Stratum 2 servers. For more information on the Network Time Protocol go to: [www.ntp.org](http://www.ntp.org)

**Examples** To stop the device from being the designated NTP server use the commands:

```
awplus# configure terminal
awplus(config)# no ntp master
```

To make the device the designated NTP server with stratum number 2 use the commands:

```
awplus# configure terminal
awplus(config)# ntp master 2
```

# ntp peer

**Overview** Use this command to configure an NTP peer association. An NTP association is a peer association if this system is willing to either synchronize to the other system, or allow the other system to synchronize to it.

NTP for IPv6 is supported in Software Version 5.4.3A-1.x and later.

Use the **no** variant of this command to remove the configured NTP peer association.

**Syntax** `ntp peer {<peeraddress>|<peername>}`  
`ntp peer {<peeraddress>|<peername>} [prefer] [key <key>]`  
`[version <version>]`  
`no ntp peer {<peeraddress>|<peername>}`

| Parameter         | Description                                                                                                                                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <peeraddress>     | Specify the IP address of the peer, entered in the form A . B . C . D for an IPv4 address, or in the form X : X : : X : X for an IPv6 address. |
| <peername>        | Specify the peer hostname. The peer hostname can resolve to an IPv4 and an IPv6 address.                                                       |
| prefer            | Prefer this peer when possible.                                                                                                                |
| key <key>         | <1-4294967295><br>Configure the peer authentication key.                                                                                       |
| version <version> | <1-4><br>Configure for this NTP version.                                                                                                       |

**Mode** Global Configuration

**Examples** See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv4 address of 192 . 0 . 2 . 23:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.2.23
awplus(config)# ntp peer 192.0.2.23 prefer
awplus(config)# ntp peer 192.0.2.23 prefer version 4
awplus(config)# ntp peer 192.0.2.23 prefer version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4
awplus(config)# ntp peer 192.0.2.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of 192.0.2.23, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 192.0.2.23
```

See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv6 address of 2001:0db8:010d::1:

```
awplus# configure terminal
awplus(config)# ntp peer 2001:0db8:010d::1
awplus(config)# ntp peer 2001:0db8:010d::1 prefer
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4 key
1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4 key 1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4
awplus(config)# ntp peer 2001:0db8:010d::1 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010d::1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 2001:0db8:010d::1
```

**Related  
Commands**   [ntp server](#)  
                  [ntp source](#)

# ntp server

**Overview** Use this command to configure an NTP server. This means that this system will synchronize to the other system, and not vice versa.

Use the **no** variant of this command to remove the configured NTP server.

**Syntax** `ntp server {<serveraddress>|<servername>}`  
`ntp server {<serveraddress>|<servername>} [prefer] [key <key>]`  
`[version <version>]`  
`no ntp server {<serveraddress>|<servername>}`

| Parameter         | Description                                                                                                                                    |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <serveraddress>   | Specify the IP address of the peer, entered in the form A . B . C . D for an IPv4 address, or in the form X : X : : X . X for an IPv6 address. |
| <servername>      | Specify the server hostname. The server hostname can resolve to an IPv4 and an IPv6 address.                                                   |
| prefer            | Prefer this server when possible.                                                                                                              |
| key <key>         | <1-4294967295><br>Configure the server authentication key.                                                                                     |
| version <version> | <1-4><br>Configure for this NTP version.                                                                                                       |

**Mode** Global Configuration

**Examples** See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv4 address of 192 . 0 . 1 . 23:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.1.23
awplus(config)# ntp server 192.0.1.23 prefer
awplus(config)# ntp server 192.0.1.23 prefer version 4
awplus(config)# ntp server 192.0.1.23 prefer version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4
awplus(config)# ntp server 192.0.1.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of 192 . 0 . 1 . 23, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp server 192.0.1.23
```

See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv6 address of 2001:0db8:010e::2:

```
awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2
awplus(config)# ntp server 2001:0db8:010e::2 prefer
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4 key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4
awplus(config)# ntp server 2001:0db8:010e::2 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010e::2, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp server 2001:0db8:010e::2
```

**Related  
Commands**    [ntp peer](#)  
                  [ntp source](#)

# ntp source

**Overview** Use this command to configure an IPv4 or an IPv6 address for the NTP source interface. This command defines the socket used for NTP messages, and only applies to NTP client behavior.

Use the **no** variant of this command to remove the configured IPv4 or IPv6 address from the NTP source interface.

**Syntax** ntp source <source-address>  
no ntp source

| Parameter        | Description                                                                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <source-address> | Specify the IP address of the NTP source interface, entered in the form A . B . C . D for an IPv4 address, or in the form X : X : : X . X for an IPv6 address. |

**Default** An IP address is selected based on the most appropriate egress interface used to reach the NTP peer if a configured NTP client source IP address is unavailable or is an invalid IP address.

**Mode** Global Configuration

**Usage** Adding an IPv4 or an IPv6 address allows you to select which source interface NTP uses for peering. The IPv4 or IPv6 address configured using this command is matched to the interface.

When selecting a source IP address to use for NTP messages to the peer, if the configured NTP client source IP address is unavailable then default behavior will apply, and an alternative source IP address is automatically selected. This IP address is based on the most appropriate egress interface used to reach the NTP peer. The configured NTP client source IP may be unavailable if the interface is down, or an invalid IP address is configured that does not reside on the device.

Note that this command only applies to NTP client behavior. The egress interface that the NTP messages use to reach the NTP server determined by the [ntp peer](#) and [ntp server](#) commands.

**Examples** To configure the NTP source interface with the IPv4 address 192 . 0 . 1 . 23, enter the commands:

```
awplus# configure terminal
awplus(config)# ntp source 192.0.1.23
```

To configure the NTP source interface with the IPv6 address 2001:0db8:010e::2, enter the commands:

```
awplus# configure terminal
awplus(config)# ntp source 2001:0db8:010e::2
```

To remove a configured address for the NTP source interface, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp source
```

**Related  
Commands**    [ntp peer](#)  
                  [ntp server](#)

## ntp trusted-key

**Overview** This command defines a list of trusted authentication keys. If a key is trusted, this system will be ready to synchronize to a system that uses this key in its NTP packets.

Use the **no** variant of this command to remove a configured trusted authentication key.

**Syntax** ntp trusted-key <1-4294967295>  
no ntp trusted-key <1-4294967295>

| Parameter      | Description              |
|----------------|--------------------------|
| <1-4294967295> | The specific key number. |

**Mode** Global Configuration

**Examples** To define a trusted authentication key numbered 234675, use the following commands:

```
awplus# configure terminal
awplus(config)# ntp trusted-key 234676
```

To remove the trusted authentication key numbered 234675, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp trusted-key 234676
```



# show counter ntp

**Overview** This command displays packet counters for NTP.

**Syntax** show counter ntp

**Mode** User Exec and Privileged Exec

**Output** Figure 37-1: Example output from the **show counter ntp** command

|                      |       |       |
|----------------------|-------|-------|
| NTP counters         |       |       |
| Pkts Sent            | ..... | 0     |
| Pkts Received        | ..... | 70958 |
| Pkts Processed       | ..... | 0     |
| Pkts current version | ..... | 0     |
| Pkts old version     | ..... | 0     |
| Pkts unknown version | ..... | 0     |
| Pkts access denied   | ..... | 70958 |
| Pkts bad length      | ..... | 0     |
| Pkts bad auth        | ..... | 0     |
| Pkts rate exceed     | ..... | 0     |

Table 37-1: Parameters in the output from the **show counter ntp** command

| Parameter            | Description                                                                                                                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pkts Sent            | Total number of NTP client and server packets sent by your device.                                                                                                                                         |
| Pkts Received        | Total number of NTP client and server packets received by your device.                                                                                                                                     |
| Pkts Processed       | The number of packets processed by NTP. NTP processes a packet once it has determined that the packet is valid by checking factors such as the packet's authentication, format, access rights and version. |
| Pkts current version | The number of version 4 NTP packets received.                                                                                                                                                              |
| Pkts old version     | The number of NTP packets received that are from an older version, down to version 1, of NTP. NTP is compatible with these versions and processes these packets.                                           |
| Pkts unknown version | The number of NTP packets received that are an earlier version than version 1, or a higher version than version 4. NTP cannot process these packets.                                                       |
| Pkts access denied   | The number of NTP packets received that do not match any access list statements in the NTP access-groups. NTP drops these packets.                                                                         |

Table 37-1: Parameters in the output from the **show counter ntp** command

| Parameter        | Description                                                                                                                                                                                                      |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Pkts bad length  | The number of NTP packets received that do not conform to the standard packet length. NTP drops these packets.                                                                                                   |
| Pkts bad auth    | The number of NTP packets received that failed authentication. NTP drops these packets. Packets can only fail authentication if NTP authentication is enabled with the <a href="#">ntp authenticate</a> command. |
| Pkts rate exceed | The number of packets dropped because the packet rate exceeded its limits.                                                                                                                                       |

**Example** To display counters for NTP, use the command:

```
awplus# show counter ntp
```

# show ntp associations

**Overview** Use this command to display the status of NTP associations. Use the detail option for displaying detailed information about the associations.

**Syntax** show ntp associations [detail]

**Mode** User Exec and Privileged Exec

**Example** See the sample output of the **show ntp associations** and **show ntp associations detail** commands displaying the status of NTP associations.

Table 37-2: Example output from the **show ntp associations** command

```
awplus#show ntp associations
address ref clock st when poll reach delay offset disp
~192.0.2.23 INIT 16 - 512 000 0.0 0.0 0.0
* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured
awplus#
```

Table 37-3: Example output from the **show ntp associations detail** command

```
awplus#show ntp associations detail
192.0.2.23 configured, sane, valid, leap_sub, stratum 16
ref ID INIT, time 00000000.00000000 (06:28:16.000 UTC Thu Feb 7 2036)
our mode client, peer mode unspec, our poll intvl 512, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 000,
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-19,
org time 00000000.00000000 (06:28:16.000 UTC Thu Feb 7 2036)
rcv time 00000000.00000000 (06:28:16.000 UTC Thu Feb 7 2036)
xmt time cf11f2a4.cedde5e4 (00:39:00.808 UTC Tue Feb 2 2010)
filtdelay = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filtoffset = 0.00 0.00 0.00 0.00 0.00 0.00 0.00 0.00
filtererror = 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00 16000.00
0 16000.00
```

Table 37-4: Parameters in the output from the **show ntp associations** command

| Parameter | Description                                                                  |
|-----------|------------------------------------------------------------------------------|
| address   | Peer IP address                                                              |
| ref clock | IP address for reference clock                                               |
| st        | Stratum. The number of hops between the server and the accurate time source. |
| poll      | Time between NTP requests from the device to the server.                     |
| reach     | Shows whether or not the NTP server responded to the last request.           |

Table 37-4: Parameters in the output from the **show ntp associations** command

| Parameter | Description                                                         |
|-----------|---------------------------------------------------------------------|
| de lay    | Round trip delay between the device and the server.                 |
| offset    | Difference between the device clock and the server clock.           |
| disp      | Lowest measure of error associated with peer offset based on delay. |

# show ntp status

**Overview** Use this command to display the status of the Network Time Protocol (NTP).

**Syntax** show ntp status

**Mode** User Exec and Privileged Exec

**Example** See the sample output of the **show ntp status** command displaying information about the Network Time Protocol.

Figure 37-2: Example output from the **show ntp status** command

```
awplus#sh ntp status
Clock is synchronized, stratum 3, reference is 127.127.1.0
actual frequency is 0.0000 Hz, precision is 2**-19
reference time is cf11f3f2.c7c081a1 (00:44:34.780 UTC Tue Feb 2
2010)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 7947729.000 msec,
awplus#
```

# 38

# Dynamic Host Configuration Protocol (DHCP) Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure DHCP.

For more information, see the [DHCP Feature Overview and Configuration Guide](#).

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](#).

- Command List**
- [“ip address dhcp”](#) on page 1279
  - [“show counter dhcp-client”](#) on page 1281
  - [“show dhcp lease”](#) on page 1282

# 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 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                                                                                                                                                                                                                            |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <interface> | 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 |
| <hostname>  | 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 a VLAN interface.

**Examples** To set the interface `vlan10` to use DHCP to obtain an IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# ip address dhcp
```

To stop the interface `vlan10` from using DHCP to obtain its IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip address dhcp
```

**Related  
Commands** [ip address](#)

**Validation**    `show running-config`  
**Commands**     `show ip interface`



# 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 “Controlling “show” Command Output” in 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 38-1: 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
DHCPOFFER in 22
DHCPACK in 18
DHCPNAK in 0
```

Table 38-1: 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.                      |
| DHCPOFFER 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 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 vlan1, use the command:

```
awplus# show dhcp lease vlan1
```

**Output** Figure 38-2: Example output from the **show dhcp lease** command

```
Interface vlan1

IP Address: 192.168.22.4
Expires: 13 Mar 2007 20:10:19
Renew: 13 Mar 2007 18:37:06
Rebind: 13 Mar 2007 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

Interface vlan2

IP Address: 100.8.16.4
Expires: 13 Mar 2007 20:15:39
Renew: 13 Mar 2007 18:42:25
Rebind: 13 Mar 2007 19:54:46
Server:
Options:
 subnet-mask 255.255.0.0
 routers 10.58.1.51
 dhcp-lease-time 1000
 dhcp-message-type 5
 dhcp-server-identifier 100.8.16.1
```

**Related  
Commands** [ip address dhcp](#)

# 39

# 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 supported in Software Version 5.4.3A-1.x and later.

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.

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](#).

**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**
- [“clear counter ipv6 dhcp-client”](#) on page 1285
  - [“clear ipv6 dhcp client”](#) on page 1286
  - [“ipv6 address dhcp”](#) on page 1287
  - [“show counter ipv6 dhcp-client”](#) on page 1288
  - [“show ipv6 dhcp”](#) on page 1290
  - [“show ipv6 dhcp interface”](#) on page 1291

# 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 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                                               |
|-------------|-----------------------------------------------------------|
| <interface> | Specify the interface name to restart a DHCPv6 client on. |

**Mode** Privileged Exec

**Example** To restart a DHCPv6 client on interface vlan1, use the following command:  
`awplus# clear ipv6 dhcp client vlan1`

# ipv6 address dhcp

**Overview** DHCPv6 is supported in Software Version 5.4.3A-1.x and later.

Use this command in Interface Configuration mode 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.

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.
- Option 15 - a domain name used to resolve host names.
- Option 51 - lease expiration time.

**Syntax** `ipv6 address dhcp`  
`no ipv6 address dhcp`

**Examples** To set the interface `vlan10` to use DHCPv6 to obtain an IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config)# ipv6 enable
awplus(config-if)# ipv6 address dhcp
```

To stop the interface `vlan10` from using DHCPv6 to obtain its IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ipv6 address dhcp
```

**Related  
Commands** [ipv6 address](#)

**Validation  
Commands** [show running-config](#)

# show counter ipv6 dhcp-client

**Overview** Use this command in User Exec or Privilege Exec mode to show DHCPv6 client counter information.

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 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 39-1: 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 39-1: 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 39-1: 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. |

# 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

**Syntax** show ipv6 dhcp

**Mode** User Exec and Privileged Exec

**Usage** 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 39-2: Example output from the **show ipv6 dhcp** command

```
awplus#show ipv6 dhcp
DHCPv6 Server DUID: 0001000117ab6876001577f7ba23
```

**Related Commands** [ipv6 address dhcp](#)

# 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 “Controlling “show” Command Output” in 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
```

**Output** Figure 39-3: Example output from the **show ipv6 dhcp interface** command

|                                              |
|----------------------------------------------|
| awplus# show ipv6 dhcp interface             |
| vlan1 is in client mode                      |
| Address 1001::3c0:1                          |
| preferred lifetime 9000, valid lifetime 5000 |
| starts at 20 Jan 2012 09:21:35               |
| expires at 20 Jan 2012 10:25:32              |

Table 39-2: Parameters in the output of the **show counter dhcp-client** command

| Parameter                     | Description                                                 |
|-------------------------------|-------------------------------------------------------------|
| <interface> is in client mode | Displays that the specified interface is in client mode.    |
| Address                       | Displays the address of the DHCPv6 server on the interface. |
| Preference                    | Displays the preference value for the DHCPv6 server.        |

# 40

# SNMP Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure SNMP. For more information, see:

- the [SNMP MIBs Overview](#), for information about which MIB objects are supported.
- the [SNMP Feature Overview and Configuration Guide](#).

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](#).

- Command List**
- “[debug snmp](#)” on page 1294
  - “[show counter snmp-server](#)” on page 1295
  - “[show debugging snmp](#)” on page 1300
  - “[show running-config snmp](#)” on page 1301
  - “[show snmp-server](#)” on page 1302
  - “[show snmp-server community](#)” on page 1303
  - “[show snmp-server group](#)” on page 1304
  - “[show snmp-server user](#)” on page 1305
  - “[show snmp-server view](#)” on page 1306
  - “[snmp trap link-status](#)” on page 1307
  - “[snmp trap link-status suppress](#)” on page 1309
  - “[snmp-server](#)” on page 1311
  - “[snmp-server community](#)” on page 1313
  - “[snmp-server contact](#)” on page 1314
  - “[snmp-server enable trap](#)” on page 1315

- [“snmp-server engineID local”](#) on page 1317
- [“snmp-server engineID local reset”](#) on page 1319
- [“snmp-server group”](#) on page 1320
- [“snmp-server host”](#) on page 1322
- [“snmp-server location”](#) on page 1324
- [“snmp-server source-interface”](#) on page 1325
- [“snmp-server startup-trap-delay”](#) on page 1326
- [“snmp-server user”](#) on page 1327
- [“snmp-server view”](#) on page 1330
- [“undebbug snmp”](#) on page 1331

# 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 40-1: 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  |
| inReadOnlyls         | ..... | 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 40-1: 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.                                                      |



Table 40-1: Parameters in the output of the **show counter snmp-server** command (cont.)

| Parameter          | Meaning                                                                                                                                                                                                                                                                                            |
|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                       |
| inReadOnlyls       | 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'.                                                                                                                                                                                          |
| 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.                                                                                                                                                                                                                   |

Table 40-1: Parameters in the output of the **show counter snmp-server** command (cont.)

| Parameter       | Meaning                                                                                                                                                                                                                              |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                                                               |
| 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.                                                                                                                                                                      |

Table 40-1: Parameters in the output of the **show counter snmp-server** command (cont.)

| Parameter            | Meaning                                                                                                                                           |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 40-2: 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 40-3: 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 40-4: 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 40-5: 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 40-6: 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 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 40-7: 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 40-8: 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** By default, link status notifications are disabled.

**Mode** Interface Configuration

**Usage** The link status notifications can be enabled for the following interface types:

- switch port (e.g. port 1.0.1)
- VLAN (e.g. vlan2)
- static and dynamic link aggregation (e.g. sa2, po2)

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 ports 1.0.2 to 1.0.6, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-1.0.6
awplus(config-if)# snmp trap link-status
```

To enable SNMP to send an Allied Telesis enterprise type of link status notification for port1.0.1, use following commands:

```
awplus# configure terminal
awplus(config)# interface 1.0.1
awplus(config-if)# snmp trap link-status enterprise
```

To disable the sending of link status notifications for port 1.0.2, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
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** 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 enable the suppression of link status notifications for ports 1.0.2 to 1.0.6 after 10 notifications have been sent in 40 seconds, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-1.0.6
awplus(config-if)# snmp trap link-status suppress time 40
threshold 10
```

To disable the suppression link status notifications for port 1.0.2, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
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 view 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|<access-list>}`  
`no snmp-server community <community-name> [{view <view-name>|<access-list>}]`

| 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.                                                                              |
| <access-list>    | <1-99> Access list number.                                                                         |

**Mode** Global Configuration

**Example** The following command creates 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
```

The following command removes 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                                                                                                                     |
|-----------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| <i>&lt;contact-info&gt;</i> | 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 device to send the specified notifications (traps).

Note that the Environmental Monitoring traps are enabled by default. So you do not need to issue this command for the Environmental Monitoring traps since these are enabled by default. SNMP environmental monitoring traps defined in AT-ENVMONv2-MIB are enabled by default.

Use the **no** variant of this command to disable the sending of the specified notifications.

**Syntax**

```
snmp-server enable trap {[auth] [dhcpsnooping]
[epsr] [lldp] [loopprot] [mstp] [nsm] [ospf] [pim]
[power-inline] [rmon] [thrash-limit]}

no snmp-server enable trap {[auth] [dhcpsnooping]
[epsr] [lldp] [loopprot] [mstp] [nsm] [ospf] [pim]
[power-inline]
[rmon] [thrash-limit]}
```

| Parameter    | Description                                                                                                                                                                                           |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| auth         | Authentication failure.                                                                                                                                                                               |
| dhcpsnooping | DHCP snooping and ARP security traps. These notifications must also be set using the <a href="#">ip dhcp snooping violation</a> command, and/or the <a href="#">arp security violation</a> command.   |
| epsr         | EPSR traps.                                                                                                                                                                                           |
| lldp         | Link Layer Discovery Protocol (LLDP) traps. These notifications must also be enabled using the <a href="#">lldp notifications</a> command, and/or the <a href="#">lldp med-notifications</a> command. |
| loopprot     | Loop Protection traps.                                                                                                                                                                                |
| mstp         | MSTP traps.                                                                                                                                                                                           |
| nsm          | NSM traps.                                                                                                                                                                                            |
| ospf         | OSPF traps.                                                                                                                                                                                           |
| pim          | PIM traps.                                                                                                                                                                                            |
| power-inline | Power-inline traps (Power Ethernet MIB RFC 3621).                                                                                                                                                     |
| rmon         | RMON traps.                                                                                                                                                                                           |
| thrash-limit | MAC address Thrash Limiting traps.                                                                                                                                                                    |

**Default** By default, no notifications are generated.

**Mode** Global Configuration

**Usage** 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 more than one trap can be configured with one command entry, and also note this command applied to notifications send by SNMP version 3.

**Examples** To enable the device to send PoE related traps, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# snmp-server enable trap power-inline
```

To disable PoE traps being sent out by the device, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no snmp-server enable power-inline
```

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
```

**Related  
Commands**

- [show snmp-server](#)
- [show ip dhcp snooping](#)
- [snmp trap link-status](#)
- [snmp-server host](#)

# 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                                                                                                                                                                                                                                                                                      |
|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <engine-id> | Specify SNMPv3 Engine ID value, a string of up to 27 characters.                                                                                                                                                                                                                                 |
| default     | 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** 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 asdgdh231234d
awplus(config)#exit
awplus#show snmp-server

SNMP Server Enabled
IP Protocol IPv4
SNMPv3 Engine ID (configured name) ... asdgdh231234d
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
```

**Validation** `show snmp-server`  
**Commands**

**Related** `snmp-server engineID local reset`  
**Commands** `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
```

**Validation  
Commands** [show snmp-server](#)

**Related  
Commands** [snmp-server engineID local](#)

## 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 <notifyname>]`  
`no snmp-server group <groupname> {auth|noauth|priv}`

| 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.                                                                      |
| <notifyname> | 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 SNMP group usergroup, use the following commands

```
awplus# configure terminal
```

```
awplus(config)# no snmp-server group usergroup noauth
```



**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 : 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.                     |

**Mode** Global Configuration

**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 command:

```
awplus# configure terminal
awplus(config)# snmp-server host version 2c public192.0.2.5
```

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 command:

```
awplus# configure terminal
awplus(config)# snmp-server host version 2c
private2001:db8::8a2e:7334
```

To remove a configured trap host of 192.0.2.5 with the SNMPv2c community name public, use the following command:

```
awplus# configure terminal
awplus(config)# no snmp-server host version 2c public192.0.2.5
```

**Related Commands**

- [snmp trap link-status](#)
- [snmp-server enable trap](#)
- [snmp-server view](#)

# 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 interface that SNMP traps or informs originate from. You cannot specify an interface that does not already have an IP address assigned to the interface.

Use the **no** variant of this command to reset to the default source interface that SNMP traps or informs originate from (the Egress interface as sent from by default).

**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 (with an IP address already assigned). |

**Default** By default the source interface is the Egress interface where traps or informs were sent from.

**Mode** Global Configuration

**Usage** An SNMP trap or inform sent from an SNMP server has the notification IP address of the interface where it was sent from. Use this command to monitor notifications from an interface.

**Example** To set the interface that SNMP informs originate from to port 1.0.2 for inform packets, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# snmp-server source-interface informs port1.0.2
```

To reset the interface to the default source interface (the Egress interface) that SNMP traps originate from for trap packets, use the following commands:

```
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                                                                   |
|---------------------------|-------------------------------------------------------------------------------|
| <i>&lt;delay-time&gt;</i> | 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** 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 des and privacy password Privpass, use the following commands

```
awplus# configure terminal
```

```
awplus(config)# snmp-server user authuser usergroup auth md5
Authpass priv des 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   | des     |

To enter existing SNMP user authuser with existing passwords as a member of group newusergroup with authentication protocol md5 plus the encrypted authentication password 0x1c74b9c22118291b0ce0cd883f8dab6b74, privacy protocol des plus the encrypted privacy password 0x0e0133db5453ebd03822b004eeacb6608f, use the following commands

```
awplus# configure terminal
```

```
awplus(config)# snmp-server user authuser newusergroup
encrypted auth md5 0x1c74b9c22118291b0ce0cd883f8dab6b74 priv
des 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   | des     |

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](#)

# undebbug snmp

**Overview** This command applies the functionality of the no [debug snmp](#) command.

# 41

# LLDP Commands

## Introduction

**Overview** LLDP and LLDP-MED can be configured using the commands in this chapter, or by using SNMP with the LLDP-MIB and LLDP-EXT-DOT1-MIB (see the [SNMP MIBs Overview](#)).

The Voice VLAN feature can be configured using commands in the [VLAN Commands](#) chapter.

For more information about LLDP, see the [LLDP Feature Overview and Configuration Guide](#).

LLDP can transmit a lot of data about the network. Typically, the network information gathered using LLDP is transferred to a Network Management System by SNMP. For security reasons, we recommend using SNMPv3 for this purpose (see the [SNMP Feature Overview and Configuration Guide](#)).

LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static or dynamic channel groups, but not on the channel groups themselves.

- Command List**
- [“clear lldp statistics”](#) on page 1334
  - [“clear lldp table”](#) on page 1335
  - [“debug lldp”](#) on page 1336
  - [“lldp faststart-count”](#) on page 1338
  - [“lldp holdtime-multiplier”](#) on page 1339
  - [“lldp management-address”](#) on page 1340
  - [“lldp med-notifications”](#) on page 1341
  - [“lldp med-tlv-select”](#) on page 1342
  - [“lldp non-strict-med-tlv-order-check”](#) on page 1344
  - [“lldp notification-interval”](#) on page 1345
  - [“lldp notifications”](#) on page 1346

- ["lldp port-number-type"](#) on page 1347
- ["lldp reinit"](#) on page 1348
- ["lldp run"](#) on page 1349
- ["lldp timer"](#) on page 1350
- ["lldp tlv-select"](#) on page 1351
- ["lldp transmit receive"](#) on page 1353
- ["lldp tx-delay"](#) on page 1354
- ["location civic-location configuration"](#) on page 1355
- ["location civic-location identifier"](#) on page 1360
- ["location civic-location-id"](#) on page 1361
- ["location coord-location configuration"](#) on page 1362
- ["location coord-location identifier"](#) on page 1364
- ["location coord-location-id"](#) on page 1365
- ["location elin-location"](#) on page 1366
- ["location elin-location-id"](#) on page 1367
- ["show debugging lldp"](#) on page 1368
- ["show lldp"](#) on page 1370
- ["show lldp interface"](#) on page 1372
- ["show lldp local-info"](#) on page 1374
- ["show lldp neighbors"](#) on page 1379
- ["show lldp neighbors detail"](#) on page 1381
- ["show lldp statistics"](#) on page 1385
- ["show lldp statistics interface"](#) on page 1387
- ["show location"](#) on page 1390

# clear lldp statistics

**Overview** This command clears all LLDP statistics (packet and event counters) associated with specified ports. If no port list is supplied, LLDP statistics for all ports are cleared.

**Syntax** `clear lldp statistics [interface <port-list>]`

| Parameter   | Description                                           |
|-------------|-------------------------------------------------------|
| <port-list> | The ports for which the statistics are to be cleared. |

**Mode** Privileged Exec

**Examples** To clear the LLDP statistics on ports 1.0.1 and 1.0.6, use the command:  
`awplus# clear lldp statistics interface port1.0.1,port1.0.6`  
To clear all LLDP statistics for all ports, use the command:  
`awplus# clear lldp statistics`

**Related Commands** [show lldp statistics](#)  
[show lldp statistics interface](#)

# clear lldp table

**Overview** This command clears the table of LLDP information received from neighbors through specified ports. If no port list is supplied, neighbor information is cleared for all ports.

**Syntax** `clear lldp table [interface <port-list>]`

| Parameter                      | Description                                                          |
|--------------------------------|----------------------------------------------------------------------|
| <code>&lt;port-list&gt;</code> | The ports for which the neighbor information table is to be cleared. |

**Mode** Privileged Exec

**Examples** To clear the table of neighbor information received on ports 1.0.1 and 1.0.6, use the command:

```
awplus# clear lldp table interface port1.0.1,port1.0.6
```

To clear the entire table of neighbor information received through all ports, use the command:

```
awplus# clear lldp table
```

**Related Commands** [show lldp neighbors](#)

# debug lldp

**Overview** This command enables specific LLDP debug for specified ports. When LLDP debugging is enabled, diagnostic messages are entered into the system log. If no port list is supplied, the specified debugging is enabled for all ports.

The **no** variant of this command disables specific LLDP debug for specified ports. If no port list is supplied, the specified debugging is disabled for all ports.

**Syntax** debug lldp {[rx][rxpkt][tx][txpkt]} [interface [<port-list>]]  
debug lldp operation  
no debug lldp {[rx][rxpkt][tx][txpkt]} [interface [<port-list>]]  
no debug lldp operation  
no debug lldp all

| Parameter   | Description                                      |
|-------------|--------------------------------------------------|
| rx          | LLDP receive debug.                              |
| rxpkt       | Raw LLDPDUs received in hex format.              |
| tx          | LLDP transmit debug.                             |
| txpkt       | Raw Tx LLDPDUs transmitted in hex format.        |
| <port-list> | The ports for which debug is to be configured.   |
| operation   | Debug for LLDP internal operation on the switch. |
| all         | Disables all LLDP debugging for all ports.       |

**Default** By default no debug is enabled for any ports.

**Mode** Privileged Exec

**Examples** To enable debugging of LLDP receive on ports 1.0.1 and 1.0.6, use the command:

```
awplus# debug lldp rx interface port1.0.1,port1.0.6
```

To enable debugging of LLDP transmit with packet dump on all ports, use the command:

```
awplus# debug lldp tx txpkt
```

To disable debugging of LLDP receive on ports 1.0.1 and 1.0.6, use the command:

```
awplus# no debug lldp rx interface port1.0.1,port1.0.6
```

To turn off all LLDP debugging on all ports, use the command:

```
awplus# no debug lldp all
```



**Related  
Commands**    `show debugging lldp`  
                  `show running-config lldp`  
                  `terminal monitor`

# lldp faststart-count

**Overview** Use this command to set the fast start count for LLDP-MED. The fast start count determines how many fast start advertisements LLDP sends from a port when it starts sending LLDP-MED advertisements from the port, for instance, when it detects a new LLDP-MED capable device.

The **no** variant of this command resets the LLDP-MED fast start count to the default (3).

**Syntax** `lldp faststart-count <1-10>`  
`no lldp faststart-count`

| Parameter | Description                                      |
|-----------|--------------------------------------------------|
| <1-10>    | The number of fast start advertisements to send. |

**Default** The default fast start count is 3.

**Mode** Global Configuration

**Examples** To set the fast start count to 5, use the command:

```
awplus# configure terminal
awplus(config)# lldp faststart-count 5
```

To reset the fast start count to the default setting (3), use the command:

```
awplus# configure terminal
awplus(config)# no lldp faststart-count
```

**Related  
Commands** [show lldp](#)

# lldp holdtime-multiplier

**Overview** This command sets the holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors.

The **no** variant of this command sets the multiplier back to its default.

**Syntax** `lldp holdtime-multiplier <2-10>`  
`no lldp holdtime-multiplier`

| Parameter | Description            |
|-----------|------------------------|
| <2-10>    | The multiplier factor. |

**Default** The default holdtime multiplier value is 4.

**Mode** Global Configuration

**Usage** The Time-To-Live defines the period for which the information advertised to the neighbor is valid. If the Time-To-Live expires before the neighbor receives another update of the information, then the neighbor discards the information from its database.

**Examples** To set the holdtime multiplier to 2, use the commands:

```
awplus# configure terminal
awplus(config)# lldp holdtime-multiplier 2
```

To set the holdtime multiplier back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp holdtime-multiplier 2
```

**Related  
Commands** [show lldp](#)

# lldp management-address

**Overview** This command sets the IPv4 address to be advertised to neighbors (in the Management Address TLV) via the specified ports. This address will override the default address for these ports.

The **no** variant of this command clears the user-configured management IP address advertised to neighbors via the specified ports. The advertised address reverts to the default.

**Syntax** `lldp management-address <ipaddr>`  
`no lldp management-address`

| Parameter                   | Description                                                                                                                                      |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;ipaddr&gt;</code> | The IPv4 address to be advertised to neighbors, in dotted decimal format. This must be one of the IP addresses already configured on the device. |

**Default** The local loopback interface primary IPv4 address if set, else the primary IPv4 interface address of the lowest numbered VLAN the port belongs to, else the MAC address of the device's baseboard if no VLAN IP addresses are configured for the port.

**Mode** Interface Configuration

**Usage** To see the management address that will be advertised, use the [show lldp interface](#) command or [show lldp local-info](#) command.

**Examples** To set the management address advertised by ports 1.0.1 and 1.0.6, to be 192.168.1.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp management-address 192.168.1.6
```

To clear the user-configured management address advertised by ports 1.0.1 and 1.0.6, and revert to using the default address, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp management-address
```

**Related Commands** [show lldp interface](#)  
[show lldp local-info](#)

# lldp med-notifications

**Overview** Use this command to enable LLDP to send LLDP-MED Topology Change Detected SNMP notifications relating to the specified ports. The switch sends an SNMP event notification when a new LLDP-MED compliant IP Telephony device is connected to or disconnected from a port on the switch.

Use the **no** variant of this command to disable the sending of LLDP-MED Topology Change Detected notifications relating to the specified ports.

**Syntax** `lldp med-notifications`  
`no lldp med-notifications`

**Default** The sending of LLDP-MED notifications is disabled by default.

**Mode** Interface Configuration

**Examples** To enable the sending of LLDP-MED Topology Change Detected notifications relating to ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp med-notifications
```

To disable the sending of LLDP-MED notifications relating to ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-notifications
```

**Related Commands** [lldp notification-interval](#)  
[lldp notifications](#)  
[snmp-server enable trap](#)  
[show lldp interface](#)

# lldp med-tlv-select

**Overview** Use this command to enable LLDP-MED Organizationally Specific TLVs for transmission in LLDP advertisements via the specified ports. The LLDP-MED Capabilities TLV must be enabled before any of the other LLDP-MED Organizationally Specific TLVs are enabled.

Use the **no** variant of this command to disable the specified LLDP-MED Organizationally Specific TLVs for transmission in LLDP advertisements via these ports. In order to disable the LLDP-MED Capabilities TLV, you must also disable the rest of these TLVs. Disabling all these TLVs disables LLDP-MED advertisements.

**Syntax** `lldp med-tlv-select {[capabilities] [network-policy] [location] [power-management-ext] [inventory-management]}`  
`lldp med-tlv-select all`  
`no lldp med-tlv-select {[capabilities] [network-policy] [location] [power-management-ext] [inventory-management]}`  
`no lldp med-tlv-select all`

| Parameter            | Description                                                                                                                                                                                                                                                                                   |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| capabilities         | LLDP-MED Capabilities TLV. When this is enabled, the MAC/PHY Configuration/Status TLV from IEEE 802.3 Organizationally Specific TLVs is also automatically included in LLDP-MED advertisements, whether or not it has been explicitly enabled by the <a href="#">lldp tlv-select</a> command. |
| network-policy       | Network Policy TLV. This TLV is transmitted if Voice VLAN parameters have been configured using the commands:                                                                                                                                                                                 |
| location             | Location Identification TLV. This TLV is transmitted if location information has been configured using the commands:                                                                                                                                                                          |
| power-management-ext | Extended Power-via-MDI TLV. This TLV is transmitted if the port is PoE capable, and PoE is enabled ( <a href="#">power-inline enable</a> command).                                                                                                                                            |
| inventory-management | Inventory Management TLV Set, including the following TLVs: <ul style="list-style-type: none"> <li>• Hardware Revision</li> <li>• Firmware Revision</li> <li>• Software Revision</li> <li>• Serial Number</li> <li>• Manufacturer Name</li> <li>• Model Name</li> <li>• Asset ID</li> </ul>   |
| all                  | All LLDP-MED Organizationally Specific TLVs.                                                                                                                                                                                                                                                  |

**Default** By default LLDP-MED Capabilities, Network Policy, Location Identification and Extended Power-via-MDI TLVs are enabled. Therefore, if LLDP is enabled using the [lldp run](#) command, by default LLDP-MED advertisements are transmitted on ports that detect LLDP-MED neighbors connected to them.

**Mode** Interface Configuration

**Usage** LLDP-MED TLVs are only sent in advertisements via a port if there is an LLDP-MED-capable device connected to it. To see whether there are LLDP-MED capable devices connected to the ports, use the [show lldp neighbors](#) command.

**Examples** To enable inclusion of the Inventory TLV Set in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp med-tlv-select inventory-management
```

To exclude the Inventory TLV Set in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-tlv-select inventory-management
```

To disable LLDP-MED advertisements transmitted via ports 1.0.1 and 1.0.6, disable all these TLVs using the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-tlv-select all
```

**Related  
Commands**

[lldp tlv-select](#)  
[location elin-location-id](#)  
[location civic-location identifier](#)  
[location civic-location configuration](#)  
[location coord-location identifier](#)  
[location coord-location configuration](#)  
[location elin-location](#)  
[show lldp interface](#)  
[switchport voice dscp](#)  
[switchport voice vlan](#)  
[switchport voice vlan priority](#)

# lldp non-strict-med-tlv-order-check

**Overview** Use this command to enable non-strict order checking for LLDP-MED advertisements it receives. That is, use this command to enable LLDP to receive and store TLVs from LLDP-MED advertisements even if they do not use standard TLV order.

Use the **no** variant of this command to disable non-strict order checking for LLDP-MED advertisements, that is, to set strict TLV order checking, so that LLDP discards any LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement.

**Syntax** `lldp non-strict-med-tlv-order-check`  
`no lldp non-strict-med-tlv-order-check`

**Default** By default TLV non-strict order checking for LLDP-MED advertisements is disabled. That is, strict order checking is applied to LLDP-MED advertisements, according to ANSI/TIA-1057, and LLDP-MED TLVs in non-standard order are discarded.

**Mode** Global Configuration

**Usage** The ANSI/TIA-1057 specifies standard order for TLVs in LLDP-MED advertisements, and specifies that if LLDP receives LLDP advertisements with non-standard LLDP-MED TLV order, the TLVs in non-standard order should be discarded. This implementation of LLDP-MED follows the standard: it transmits TLVs in the standard order, and by default discards LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement. However, some implementations of LLDP transmit LLDP-MED advertisements with non-standard TLV order. To receive and store the data from these non-standard advertisements, enable non-strict order checking for LLDP-MED advertisements using this command.

**Examples** To enable strict TLV order checking, use the commands:

```
awplus# configure terminal
awplus(config)# lldp tlv-order-check
```

To disable strict TLV order checking, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp tlv-order-check
```

**Related Commands** [show running-config lldp](#)



# lldp notification-interval

**Overview** This command sets the notification interval. This is the minimum interval between LLDP SNMP notifications (traps) of each kind (LLDP Remote Tables Change Notification and LLDP-MED Topology Change Notification).

The **no** variant of this command sets the notification interval back to its default.

**Syntax** `lldp notification-interval <5-3600>`  
`no lldp notification-interval`

| Parameter  | Description              |
|------------|--------------------------|
| <5 - 3600> | The interval in seconds. |

**Default** The default notification interval is 5 seconds.

**Mode** Global Configuration

**Examples** To set the notification interval to 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp notification-interval 20
```

To set the notification interval back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp notification-interval
```

**Related  
Commands** [lldp notifications](#)  
[show lldp](#)

# lldp notifications

**Overview** This command enables the sending of LLDP SNMP notifications (traps) relating to specified ports.

The **no** variant of this command disables the sending of LLDP SNMP notifications for specified ports.

**Syntax** lldp notifications  
no lldp notifications

**Default** The sending of LLDP SNMP notifications is disabled by default.

**Mode** Interface Configuration

**Examples** To enable sending of LLDP SNMP notifications for ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp notifications
```

To disable sending of LLDP SNMP notifications for ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp notifications
```

**Related Commands** lldp notification-interval  
show lldp interface  
snmp-server enable trap

# lldp port-number-type

**Overview** This command sets the type of port identifier used to enumerate, that is to count, the LLDP MIB local port entries. The LLDP MIB (IEEE Standard 802.1AB-2005, Section 12, LLDP MIB Definitions.) requires the port number value to count LLDP local port entries.

This command also enables you to optionally set an interface index to enumerate the LLDP MIB local port entries, if required by your management system.

The **no** variant of this command resets the type of port identifier back to the default setting (number).

**Syntax** `lldp port-number-type [number|ifindex]`  
`no lldp port-number-type`

| Parameter | Description                                                                                         |
|-----------|-----------------------------------------------------------------------------------------------------|
| number    | Set the type of port identifier to a port number to enumerate the LLDP MIB local port entries.      |
| ifindex   | Set the type of port identifier to an interface index to enumerate the LLDP MIB local port entries. |

**Default** The default port identifier type is number. The no variant of this command sets the port identifier type to the default.

**Mode** Global Configuration

**Examples** To set the type of port identifier used to enumerate LLDP MIB local port entries to port numbers, use the commands:

```
awplus# configure terminal
awplus(config)# lldp port-number-type number
```

To set the type of port identifier used to enumerate LLDP MIB local port entries to interface indexes, use the commands:

```
awplus# configure terminal
awplus(config)# lldp port-number-type ifindex
```

To reset the type of port identifier used to enumerate LLDP MIB local port entries the default (port numbers), use the commands:

```
awplus# configure terminal
awplus(config)# no lldp port-number-type
```

**Related Commands** [show lldp](#)

# lldp reinit

**Overview** This command sets the value of the reinitialization delay. This is the minimum time after disabling LLDP on a port before it can reinitialize.

The **no** variant of this command sets the reinitialization delay back to its default setting.

**Syntax** `lldp reinit <1-10>`  
`no lldp reinit`

| Parameter | Description           |
|-----------|-----------------------|
| <1-10>    | The delay in seconds. |

**Default** The default reinitialization delay is 2 seconds.

**Mode** Global Configuration

**Examples** To set the reinitialization delay to 3 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp reinit 3
```

To set the reinitialization delay back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp reinit
```

**Related  
Commands** [show lldp](#)

# lldp run

**Overview** This command enables the operation of LLDP on the device.  
The **no** variant of this command disables the operation of LLDP on the device. The LLDP configuration remains unchanged.

**Syntax** lldp run  
no lldp run

**Default** LLDP is disabled by default.

**Mode** Global Configuration

**Examples** To enable LLDP operation, use the commands:

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

To disable LLDP operation, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp run
```

**Related  
Commands** [show lldp](#)

# lldp timer

**Overview** This command sets the value of the transmit interval. This is the interval between regular transmissions of LLDP advertisements.

The **no** variant of this command sets the transmit interval back to its default.

**Syntax** `lldp timer <5-32768>`  
`no lldp timer`

| Parameter | Description                                                                                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <5-32768> | The transmit interval in seconds. The transmit interval must be at least four times the transmission delay timer ( <a href="#">lldp tx-delay</a> command). |

**Default** The default transmit interval is 30 seconds.

**Mode** Global Configuration

**Examples** To set the transmit interval to 90 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp timer 90
```

To set the transmit interval back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp timer
```

**Related  
Commands** [lldp tx-delay](#)  
[show lldp](#)

# lldp tlv-select

**Overview** This command enables one or more optional TLVs, or all TLVs, for transmission in LLDP advertisements via the specified ports. The TLVs can be specified in any order; they are placed in LLDP frames in a fixed order (as described in IEEE 802.1AB). The mandatory TLVs (Chassis ID, Port ID, Time To Live, End of LLDPDU) are always included in LLDP advertisements.

In LLDP-MED advertisements the MAC/PHY Configuration/Status TLV will be always be included regardless of whether it is selected by this command.

The **no** variant of this command disables the specified optional TLVs, or all optional TLVs, for transmission in LLDP advertisements via the specified ports.

**Syntax** `lldp tlv-select {[<tlv>]...}`  
`lldp tlv-select all`  
`no lldp tlv-select {[<tlv>]...}`  
`no lldp tlv-select all`

| Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <tlv>     | The TLV to transmit in LLDP advertisements. One of these keywords: <ul style="list-style-type: none"><li>• port-description (specified by the <a href="#">description (interface)</a> command)</li><li>• system-name (specified by the <a href="#">hostname</a> command)</li><li>• system-description</li><li>• system-capabilities</li><li>• management-address</li><li>• port-vlan</li><li>• port-and-protocol-vlans</li><li>• vlan-names</li><li>• protocol-ids</li><li>• mac-phy-config</li><li>• power-management (Power Via MDI TLV)</li><li>• link-aggregation</li><li>• max-frame-size</li></ul> |
| all       | All TLVs.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

**Default** By default no optional TLVs are included in LLDP advertisements. The MAC/PHY Configuration/Status TLV ( **mac-phy-config**) is included in LLDP-MED advertisements whether or not it is selected by this command.

**Mode** Interface Configuration

**Examples** To include the management-address and system-name TLVs in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp tlv-select management-address
system-name
```

To include all optional TLVs in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp tlv-select all
```

To exclude the management-address and system-name TLVs from advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp tlv-select management-address
system-name
```

To exclude all optional TLVs from advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp tlv-select all
```

**Related  
Commands**

- [description \(interface\)](#)
- [hostname](#)
- [lldp med-tlv-select](#)
- [show lldp interface](#)
- [show lldp local-info](#)



# lldp transmit receive

**Overview** This command enables transmission and/or reception of LLDP advertisements to or from neighbors through the specified ports.

The **no** variant of this command disables transmission and/or reception of LLDP advertisements through specified ports.

**Syntax** `lldp {[transmit] [receive]}`  
`no lldp {[transmit] [receive]}`

| Parameter | Description                                                                   |
|-----------|-------------------------------------------------------------------------------|
| transmit  | Enable or disable transmission of LLDP advertisements via this port or ports. |
| receive   | Enable or disable reception of LLDP advertisements via this port or ports.    |

**Default** LLDP advertisement transmission and reception are enabled on all ports by default.

**Mode** Interface Configuration

**Examples** To enable transmission of LLDP advertisements on ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp transmit
```

To enable LLDP advertisement transmission and reception on ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp transmit receive
```

To disable LLDP advertisement transmission and reception on ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp transmit receive
```

**Related Commands** [show lldp interface](#)

# lldp tx-delay

**Overview** This command sets the value of the transmission delay timer. This is the minimum time interval between transmitting LLDP advertisements due to a change in LLDP local information.

The **no** variant of this command sets the transmission delay timer back to its default setting.

**Syntax** `lldp tx-delay <1-8192>`  
`no lldp tx-delay`

| Parameter                   | Description                                                                                                                                                |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>&lt;1-8192&gt;</code> | The transmission delay in seconds. The transmission delay cannot be greater than a quarter of the transmit interval ( <a href="#">lldp timer</a> command). |

**Default** The default transmission delay timer is 2 seconds.

**Mode** Global Configuration

**Examples** To set the transmission delay timer to 12 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp tx-delay 12
```

To set the transmission delay timer back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp tx-delay
```

**Related  
Commands** [lldp timer](#)  
[show lldp](#)

# location civic-location configuration

**Overview** Use these commands to configure a civic address location. The country parameter must be specified first, and at least one of the other parameters must be configured before the location can be assigned to a port.

Use the **no** variants of this command to delete civic address parameters from the location.

**Syntax** country <country>  
state <state>  
no state  
county <county>  
no county  
city <city>  
no city  
division <division>  
no division  
neighborhood <neighborhood>  
no neighborhood  
street-group <street-group>  
no street-group  
leading-street-direction <leading-street-direction>  
no leading-street-direction  
trailing-street-suffix <trailing-street-suffix>  
no trailing-street-suffix  
street-suffix <street-suffix>  
no street-suffix  
house-number <house-number>  
no house-number  
house-number-suffix <house-number-suffix>  
no house-number-suffix  
landmark <landmark>  
no landmark  
additional-information <additional-information>  
no additional-information  
name <name>  
no name  
postalcode <postalcode>  
no postalcode  
building <building>  
no building  
unit <unit>  
no unit  
floor <floor>  
no floor  
room <room>

```

no room
place-type <place-type>
no place-type
postal-community-name <postal-community-name>
no postal-community-name
post-office-box <post-office-box>
no post-office-box
additional-code <additional-code>
no additional-code
seat <seat>
no seat
primary-road-name <primary-road-name>
no primary-road-name
road-section <road-section>
no road-section
branch-road-name <branch-road-name>
no branch-road-name
sub-branch-road-name <sub-branch-road-name>
no sub-branch-road-name
street-name-pre-modifier <street-name-pre-modifier>
no street-name-pre-modifier
streetname-post-modifier <streetname-post-modifier>
no streetname-post-modifier

```

| Parameter                  | Description                                                                        |
|----------------------------|------------------------------------------------------------------------------------|
| <country>                  | Upper-case two-letter country code, as specified in ISO 3166.                      |
| <state>                    | State (Civic Address (CA) Type 1): national subdivisions (state, canton, region).  |
| <county>                   | County (CA Type 2): County, parish, gun (JP), district (IN).                       |
| <city>                     | City (CA Type 3): city, township, shi (JP).                                        |
| <division>                 | City division (CA Type 4): City division, borough, city district, ward, chou (JP). |
| <neighborhood>             | Neighborhood (CA Type 5): neighborhood, block.                                     |
| <street-group>             | Street group (CA Type 6): group of streets below the neighborhood level.           |
| <leading-street-direction> | Leading street direction (CA Type 16).                                             |

| Parameter                                      | Description                                           |
|------------------------------------------------|-------------------------------------------------------|
| <code>&lt;trailing-street-suffix&gt;</code>    | Trailing street suffix (CA Type 17).                  |
| <code>&lt;street-suffix&gt;</code>             | Street suffix (CA Type 18): street suffix or type.    |
| <code>&lt;house-number&gt;</code>              | House number (CA Type 19).                            |
| <code>&lt;house-number-suffix&gt;</code>       | House number suffix (CA Type 20).                     |
| <code>&lt;landmark&gt;</code>                  | Landmark or vanity address (CA Type 21).              |
| <code>&lt;additional-information&gt;</code>    | Additional location information (CA Type 22).         |
| <code>&lt;name&gt;</code>                      | Name (CA Type 23): residence and office occupant.     |
| <code>&lt;postal-code&gt;</code>               | Postal/zip code (CA Type 24).                         |
| <code>&lt;building&gt;</code>                  | Building (CA Type 25): structure.                     |
| <code>&lt;unit&gt;</code>                      | Unit (CA Type 26): apartment, suite.                  |
| <code>&lt;floor&gt;</code>                     | Floor (CA Type 27).                                   |
| <code>&lt;room&gt;</code>                      | Room (CA Type 28).                                    |
| <code>&lt;place-type&gt;</code>                | Type of place (CA Type 29).                           |
| <code>&lt;postal-community-name&gt;</code>     | Postal community name (CA Type 30).                   |
| <code>&lt;post-office-box&gt;</code>           | Post office box (P.O. Box) (CA Type 31).              |
| <code>&lt;additional-code&gt;</code>           | Additional code (CA Type 32).                         |
| <code>&lt;seat&gt;</code>                      | Seat (CA Type 33): seat (desk, cubicle, workstation). |
| <code>&lt;primary-road-name&gt;</code>         | Primary road name (CA Type 34).                       |
| <code>&lt;road-section&gt;</code>              | Road section (CA Type 35).                            |
| <code>&lt;branch-road-name&gt;</code>          | Branch road name (CA Type 36).                        |
| <code>&lt;sub-branch-road-name&gt;</code>      | Sub-branch road name (CA Type 37).                    |
| <code>&lt;street-name-pre-modifier&gt;</code>  | Street name pre-modifier (CA Type 38).                |
| <code>&lt;street-name-post-modifier&gt;</code> | Street name post-modifier (CA Type 39).               |

**Default** By default no civic address location information is configured.

**Mode** Civic Address Location Configuration

**Usage** The **country** parameter must be configured before any other parameters can be configured; this creates the location. The country parameter cannot be deleted. One or more of the other parameters must be configured before the location can be assigned to a port. The country parameter must be entered as an upper-case two-letter country code, as specified in ISO 3166. All other parameters are entered as alpha-numeric strings. Do not configure all the civic address parameters (this would generate TLVs that are too long). Configure a subset of these

parameters—enough to consistently and precisely identify the location of the device. If the location is to be used for Emergency Call Service (ECS), the particular ECS application may have guidelines for configuring the civic address location. For more information about civic address format, see the [LLDP Feature Overview and Configuration Guide](#).

To specify the civic address location, use the [location civic-location identifier](#) command. To delete the civic address location, use the **no** variant of the **location civic-location identifier** command. To assign the civic address location to particular ports, so that it can be advertised in TLVs from those ports, use the command [location civic-location-id](#) command.

**Examples** To configure civic address location 1 with location "27 Nazareth Avenue, Christchurch, New Zealand" in civic-address format, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)# country NZ
awplus(config-civic)# city Christchurch
awplus(config-civic)# primary-road-name Nazareth
awplus(config-civic)# street-suffix Avenue
awplus(config-civic)# house-number 27
```

**Related Commands**

- [location civic-location-id](#)
- [location civic-location identifier](#)
- [show lldp local-info](#)
- [show location](#)

# location civic-location identifier

**Overview** Use this command to enter the Civic Address Location Configuration mode to configure the specified location.

Use the **no** variant of this command to delete a civic address location. This also removes the location from any ports it has been assigned to.

**Syntax** location civic-location identifier <civic-loc-id>  
no location civic-location identifier <civic-loc-id>

| Parameter      | Description                                                 |
|----------------|-------------------------------------------------------------|
| <civic-loc-id> | A unique civic address location ID, in the range 1 to 4095. |

**Default** By default there are no civic address locations.

**Mode** Global Configuration

**Usage** To configure the location information for this civic address location identifier, use the [location civic-location configuration](#) command. To associate this civic location identifier with particular ports, use the [location elin-location-id](#) command.

Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

**Examples** To enter Civic Address Location Configuration mode for the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)#
```

To delete the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location civic-location identifier 1
```

**Related Commands** [location civic-location-id](#)  
[location civic-location configuration](#)  
[show location](#)  
[show running-config lldp](#)



# location civic-location-id

**Overview** Use this command to assign a civic address location to the ports. The civic address location must already exist. This replaces any previous assignment of civic address location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location identifier from the ports.

**Syntax** location civic-location-id <civic-loc-id>  
no location civic-location-id [<civic-loc-id>]

| Parameter      | Description                                        |
|----------------|----------------------------------------------------|
| <civic-loc-id> | Civic address location ID, in the range 1 to 4095. |

**Default** By default no civic address location is assigned to ports.

**Mode** Interface Configuration

**Usage** The civic address location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, create the location using the following commands:

- [location civic-location identifier](#) command
- [location civic-location configuration](#) command

If a civic-address location is deleted using the **no** variant of the [location civic-location identifier](#) command, it is automatically removed from all ports.

**Examples** To assign the civic address location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location civic-location-id 1
```

To remove a civic address location from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location civic-location-id
```

**Related Commands** [lldp med-tlv-select](#)  
[location civic-location identifier](#)  
[location civic-location configuration](#)  
[show location](#)

# location coord-location configuration

**Overview** Use this command to configure a coordinate-based location. All parameters must be configured before assigning this location identifier to a port.

**Syntax** latitude <latitude>  
lat-resolution <lat-resolution>  
longitude <longitude>  
long-resolution <long-resolution>  
altitude <altitude> {meters|floor}  
alt-resolution <alt-resolution>  
datum {wgs84|nad83-navd|nad83-mllw}

| Parameter         | Description                                                                                                                       |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| <lat-resolution>  | Latitude resolution, as a number of valid bits, in the range 0 to 34.                                                             |
| <latitude>        | Latitude value in degrees in the range -90.0 to 90.0                                                                              |
| <long-resolution> | Longitude resolution, as a number of valid bits, in the range 0 to 34.                                                            |
| <longitude>       | Longitude value in degrees, in the range -180.0 to 180.0.                                                                         |
| <alt-resolution>  | Altitude resolution, as a number of valid bits, in the range 0 to 30. A resolution of 0 can be used to indicate an unknown value. |
| <altitude>        | Altitude value, in meters or floors.                                                                                              |
| meters            | The altitude value is in meters.                                                                                                  |
| floors            | The altitude value is in floors.                                                                                                  |
| datum             | The geodetic system (or datum) that the specified coordinate values are based on.                                                 |
| wgs84             | World Geodetic System 1984.                                                                                                       |
| nad83-navd        | North American Datum 1983 - North American Vertical Datum.                                                                        |
| nad83-mllw        | North American Datum 1983 - Mean Lower Low Water vertical datum.                                                                  |

**Default** By default no coordinate location information is configured.

**Mode** Coordinate Configuration

**Usage** Latitude and longitude values are always stored internally, and advertised in the Location Identification TLV, as 34-bit fixed-point binary numbers, with a 25-bit fractional part, irrespective of the number of digits entered by the user. Likewise

altitude is stored as a 30-bit fixed point binary number, with an 8-bit fractional part. Because the user-entered decimal values are stored as fixed point binary numbers, they cannot always be represented exactly—the stored binary number is converted to a decimal number for display in the output of the [show location](#) command. For example, a user-entered latitude value of “2.77” degrees is displayed as “2.7699999809265136718750000”.

The **lat-resolution**, **long-resolution**, and **alt-resolution** parameters allow the user to specify the resolution of each coordinate element as the number of valid bits in the internally-stored binary representation of the value. These resolution values can be used by emergency services to define a search area.

To specify the coordinate identifier, use the [location coord-location identifier](#) command. To remove coordinate information, delete the coordinate location by using the **no** variant of that command. To associate the coordinate location with particular ports, so that it can be advertised in TLVs from those ports, use the [location elin-location-id](#) command.

**Example** To configure the location for the White House in Washington DC, which has the coordinates based on the WGS84 datum of 38.89868 degrees North (with 22 bit resolution), 77.03723 degrees West (with 22 bit resolution), and 15 meters height (with 9 bit resolution), use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)# la-resolution 22
awplus(config-coord)# latitude 38.89868
awplus(config-coord)# lo-resolution 22
awplus(config-coord)# longitude -77.03723
awplus(config-coord)# alt-resolution 9
awplus(config-coord)# altitude 15 meters
awplus(config-coord)# datum wgs84
```

**Related Commands**

- [location coord-location-id](#)
- [location coord-location identifier](#)
- [show lldp local-info](#)
- [show location](#)

# location coord-location identifier

**Overview** Use this command to enter Coordinate Location Configuration mode for this coordinate location.

Use the **no** variant of this command to delete a coordinate location. This also removes the location from any ports it has been assigned to.

**Syntax** location coord-location identifier *<coord-loc-id>*  
no location coord-location identifier *<coord-loc-id>*

| Parameter                   | Description                                                      |
|-----------------------------|------------------------------------------------------------------|
| <i>&lt;coord-loc-id&gt;</i> | A unique coordinate location identifier, in the range 1 to 4095. |

**Default** By default there are no coordinate locations.

**Mode** Global Configuration

**Usage** Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

To configure this coordinate location, use the [location coord-location configuration](#) command. To associate this coordinate location with particular ports, so that it can be advertised in TLVs from those ports, use the [location coord-location-id](#) command.

**Examples** To enter Coordinate Location Configuration mode to configure the coordinate location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)#
```

To delete coordinate location 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location coord-location identifier 1
```

**Related Commands** [location coord-location-id](#)  
[location coord-location configuration](#)  
[show lldp local-info](#)  
[show location](#)

# location coord-location-id

**Overview** Use this command to assign a coordinate location to the ports. The coordinate location must already exist. This replaces any previous assignment of coordinate location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location from the ports.

**Syntax** location coord-location-id <coord-loc-id>  
no location coord-location-id [<coord-loc-id>]

| Parameter      | Description                                     |
|----------------|-------------------------------------------------|
| <coord-loc-id> | Coordinate location ID, in the range 1 to 4095. |

**Default** By default no coordinate location is assigned to ports.

**Mode** Interface Configuration

**Usage** The coordinate location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, configure the location using the following commands:

- [location coord-location identifier](#) command
- [location coord-location configuration](#) command

If a coordinate location is deleted using the **no** variant of the [location coord-location identifier](#) command, it is automatically removed from all ports.

**Examples** To assign coordinate location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location coord-location-id 1
```

To remove a coordinate location from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location coord-location-id
```

**Related Commands** [lldp med-tlv-select](#)  
[location coord-location identifier](#)  
[location coord-location configuration](#)  
[show location](#)

# location elin-location

**Overview** Use this command to create or modify an ELIN location.

Use the **no** variant of this command to delete an ELIN location, and remove it from any ports it has been assigned to.

**Syntax** `location elin-location <elin> identifier <elin-loc-id>`  
`no location elin-location identifier <elin-loc-id>`

| Parameter     | Description                                                                                                                                                                |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <elin>        | Emergency Location Identification Number (ELIN) for Emergency Call Service (ECS), in the range 10 to 25 digits long. In North America, ELINs are typically 10 digits long. |
| <elin-loc-id> | A unique ELIN location identifier, in the range 1 to 4095.                                                                                                                 |

**Default** By default there are no ELIN location identifiers.

**Mode** Global Configuration

**Usage** Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

To assign this ELIN location to particular ports, so that it can be advertised in TLVs from those ports, use the [location elin-location-id](#) command.

**Examples** To create a new ELIN location with ID 1, and configure it with ELIN "1234567890", use the commands:

```
awplus# configure terminal
```

```
awplus(config)# location elin-location 1234567890 identifier 1
```

To delete existing ELIN location with ID 1, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no location elin-location identifier 1
```

**Related Commands** [location elin-location-id](#)  
[show lldp local-info](#)  
[show location](#)

# location elin-location-id

**Overview** Use this command to assign an ELIN location to the ports. The ELIN location must already exist. This replaces any previous assignment of ELIN location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location identifier from the ports.

**Syntax** location elin-location-id <elin-loc-id>  
no location elin-location-id [<elin-loc-id>]

| Parameter     | Description                                       |
|---------------|---------------------------------------------------|
| <elin-loc-id> | ELIN location identifier, in the range 1 to 4095. |

**Default** By default no ELIN location is assigned to ports.

**Mode** Interface Configuration

**Usage** An ELIN location associated with a port can be transmitted in Location Identification TLVs via the port.  
Before using this command, configure the location using the [location elin-location](#) command.

If an ELIN location is deleted using the **no** variant of one of the [location elin-location](#) command, it is automatically removed from all ports.

**Examples** To assign ELIN location 1 to port 1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location elin-location-id 1
```

To remove an ELIN location from port 1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location elin-location-id
```

**Related Commands** [lldp med-tlv-select](#)  
[location elin-location](#)  
[show location](#)

# show debugging lldp

**Overview** This command displays LLDP debug settings for specified ports. If no port list is supplied, LLDP debug settings for all ports are displayed.

**Syntax** show debugging lldp [interface <port-list>]

| Parameter   | Description                                            |
|-------------|--------------------------------------------------------|
| <port-list> | The ports for which the LLDP debug settings are shown. |

**Mode** User Exec and Privileged Exec

**Examples** To display LLDP debug settings for all ports, use the command:

```
awplus# show debugging lldp
```

To display LLDP debug settings for ports 1.0.1 to 1.0.6, use the command:

```
awplus# show debugging lldp interface port1.0.1-1.0.6
```

**Output** Figure 41-1: Example output from the **show debugging lldp** command

| LLDP Debug settings:<br>Debugging for LLDP internal operation is on |     |       |     |       |
|---------------------------------------------------------------------|-----|-------|-----|-------|
| Port                                                                | Rx  | RxPkt | Tx  | TxPkt |
| -----                                                               |     |       |     |       |
| 1.0.1                                                               | Yes | Yes   | No  | No    |
| 1.0.2                                                               | Yes | No    | No  | No    |
| 1.0.3                                                               | No  | No    | No  | No    |
| 1.0.4                                                               | Yes | Yes   | Yes | No    |
| 1.0.5                                                               | Yes | No    | Yes | No    |
| 1.0.6                                                               | Yes | Yes   | Yes | Yes   |

Table 41-1: Parameters in the output of the **show debugging lldp** command

| Parameter | Description                                                            |
|-----------|------------------------------------------------------------------------|
| Port      | Port name.                                                             |
| Rx        | Whether debugging of LLDP receive is enabled on the port.              |
| RxPkt     | Whether debugging of LLDP receive packet dump is enabled on the port.  |
| Rx        | Whether debugging of LLDP transmit is enabled on the port.             |
| RxPkt     | Whether debugging of LLDP transmit packet dump is enabled on the port. |



**Related  
Commands** [debug lldp](#)

# show lldp

**Overview** This command displays LLDP status and global configuration settings.

**Syntax** show lldp

**Mode** User Exec and Privileged Exec

**Example** To display LLDP status and global configuration settings, use the command:

```
awplus# show lldp
```

## Output

Table 41-2: Example output from the **show lldp** command

```
awplus# show lldp

LLDP Global Configuration: [Default Values]
LLDP Status Enabled [Disabled]
Notification Interval 5 secs [5]
Tx Timer Interval 30 secs [30]
Hold-time Multiplier 4 [4]
(Computed TTL value 120 secs)
Reinitialization Delay 2 secs [2]
Tx Delay 2 secs [2]

Port Number Type..... Ifindex [Port-Number]
Fast Start Count 5 [3]

LLDP Global Status:
Total Neighbor Count 47
Neighbors table last updated 0 hrs 0 mins 43 secs ago
```

Table 41-3: Parameters in the output of the **show lldp** command

| Parameter              | Description                                                                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LLDP Status            | Whether LLDP is enabled. Default is disabled.                                                                                                                 |
| Notification Interval  | Minimum interval between LLDP notifications.                                                                                                                  |
| Tx Timer Interval      | Transmit interval between regular transmissions of LLDP advertisements.                                                                                       |
| Hold-time Multiplier   | The holdtime multiplier. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors. |
| Reinitialization Delay | The reinitialization delay. This is the minimum time after disabling LLDP transmit on a port before it can reinitialize again.                                |

Table 41-3: Parameters in the output of the **show lldp** command (cont.)

| Parameter                    | Description                                                                                                                              |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Tx Delay                     | The transmission delay. This is the minimum time interval between transmitting advertisements due to a change in LLDP local information. |
| Port Number Type             | The type of port identifier used to enumerate LLDP MIB local port entries, as set by the lldp port-number-type command.                  |
| Fast Start Count             | The number of times fast start advertisements are sent for LLDP-MED.                                                                     |
| Total Neighbor Count         | Number of LLDP neighbors discovered on all ports.                                                                                        |
| Neighbors table last updated | The time since the LLDP neighbor table was last updated.                                                                                 |

**Related Commands** [show lldp interface](#)  
[show running-config lldp](#)

# show lldp interface

**Overview** This command displays LLDP configuration settings for specified ports. If no port list is specified, LLDP configuration for all ports is displayed.

**Syntax** show lldp interface [*<port-list>*]

| Parameter                | Description                                                          |
|--------------------------|----------------------------------------------------------------------|
| <i>&lt;port-list&gt;</i> | The ports for which the LLDP configuration settings are to be shown. |

**Mode** User Exec and Privileged Exec

**Examples** To display LLDP configuration settings for ports 1.0.1 to 1.0.6, use the command:

```
awplus# show lldp interface port1.0.1-1.0.6
```

To display LLDP configuration settings for all ports, use the command:

```
awplus# show lldp interface
```

**Output** Figure 41-2: Example output from the **show lldp interface** command

```
awplus# show lldp interface port1.0.1-1.0.6
LLDP Port Status and Configuration:
```

\* = LLDP is inactive on this port because it is a mirror analyser port

Notification Abbreviations:

RC = LLDP Remote Tables Change      TC = LLDP-MED Topology Change

TLV Abbreviations:

Base: Pd = Port Description      Sn = System Name  
       Sd = System Description     Sc = System Capabilities  
       Ma = Management Address

802.1: Pv = Port VLAN ID      Pp = Port And Protocol VLAN ID  
       Vn = VLAN Name          Pi = Protocol Identity

802.3: Mp = MAC/PHY Config/Status   Po = Power Via MDI (PoE)  
       La = Link Aggregation        Mf = Maximum Frame Size

MED: Mc = LLDP-MED Capabilities   Np = Network Policy  
       Lo = Location Identification   Pe = Extended PoE    In = Inventory

| Port   | Rx/Tx | Notif | Management Addr | Optional TLVs Enabled for Tx |          |       |            |
|--------|-------|-------|-----------------|------------------------------|----------|-------|------------|
|        |       |       |                 | Base                         | 802.1    | 802.3 | MED        |
| 1.0.1  | Rx Tx | RC -- | 192.168.100.123 | PdSnSdScMa                   | -----    | ----- | McNpLoPe-- |
| *1.0.2 | -- Tx | RC -- | 192.168.100.123 | PdSnSdScMa                   | -----    | ----- | McNpLoPe-- |
| 1.0.3  | Rx Tx | RC -- | 192.168.100.123 | Pd--SdScMa                   | PvPpVnPi | ----- | McNpLoPe-- |
| 1.0.4  | -- -- | RC -- | 192.168.100.123 | PdSnSd--Ma                   | -----    | ----- | McNpLoPe-- |
| 1.0.5  | Rx Tx | RC TC | 192.168.100.123 | PdSnSdScMa                   | PvPpVnPi | ----- | McNpLoPe-- |
| 1.0.6  | Rx Tx | RC TC | 192.168.100.123 | Pd----ScMa                   | -----    | ----- | McNpLoPe-- |

Table 41-4: Parameters in the output of the **show lldp interface** command

| Parameter                 | Description                                                                                                                                                                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Port                      | Port name.                                                                                                                                                                                                                                                          |
| Rx                        | Whether reception of LLDP advertisements is enabled on the port.                                                                                                                                                                                                    |
| Tx                        | Whether transmission of LLDP advertisements is enabled on the port.                                                                                                                                                                                                 |
| Notif                     | Whether sending SNMP notification for LLDP is enabled on the port: <ul style="list-style-type: none"> <li>RM = Remote Tables Change Notification</li> <li>TP = LLDP-MED Topology Change Notification</li> </ul>                                                     |
| Management Addr           | Management address advertised to neighbors.                                                                                                                                                                                                                         |
| Base TLVs Enabled for Tx  | List of optional Base TLVs enabled for transmission: <ul style="list-style-type: none"> <li>Pd = Port Description</li> <li>Sn = System Name</li> <li>Sd = System Description</li> <li>Sc = System Capabilities</li> <li>Ma = Management Address</li> </ul>          |
| 802.1 TLVs Enabled for Tx | List of optional 802.1 TLVs enabled for transmission: <ul style="list-style-type: none"> <li>Pv = Port VLAN ID</li> <li>Pp = Port And Protocol VLAN ID</li> <li>Vn = VLAN Name</li> <li>Pi = Protocol Identity</li> </ul>                                           |
| 802.3 TLVs Enabled for Tx | List of optional 802.3 TLVs enabled for transmission: <ul style="list-style-type: none"> <li>Mp = MAC/PHY Configuration/Status</li> <li>Po = Power Via MDI (PoE)</li> <li>La = Link Aggregation</li> <li>Mf = Maximum Frame Size</li> </ul>                         |
| MED TLVs Enabled for Tx   | List of optional LLDP-MED TLVs enabled for transmission: <ul style="list-style-type: none"> <li>Mc = LLDP-MED Capabilities</li> <li>Np = Network Policy</li> <li>Lo = Location Information,</li> <li>Pe = Extended Power-Via-MDI</li> <li>In = Inventory</li> </ul> |

**Related Commands** [show lldp](#)  
[show running-config lldp](#)

# show lldp local-info

**Overview** This command displays local LLDP information that can be transmitted through specified ports. If no port list is entered, local LLDP information for all ports is displayed.

**Syntax** `show lldp local-info [base] [dot1] [dot3] [med] [interface <port-list>]`

| Parameter   | Description                                               |
|-------------|-----------------------------------------------------------|
| base        | Information for base TLVs.                                |
| dot1        | Information for 802.1 TLVs.                               |
| dot3        | Information for 802.3 TLVs.                               |
| med         | Information for LLDP-MED TLVs.                            |
| <port-list> | The ports for which the local information is to be shown. |

**Mode** User Exec and Privileged Exec

**Usage** Whether and which local information is transmitted in advertisements via a port depends on:

- whether the port is set to transmit LLDP advertisements ([lldp transmit receive](#) command)
- which TLVs it is configured to send ([lldp tlv-select](#) command, [lldp med-tlv-select](#) command)

**Examples** To display local information transmitted via port 1.0.1, use the command:

```
awplus# show lldp local-info interface port1.0.1
```

To display local information transmitted via all ports, use the command:

```
awplus# show lldp local-info
```

**Output** Figure 41-3: Example output from **show lldp local-info**

```

LLDP Local Information:

Local port1.0.1:
 Chassis ID Type MAC address
 Chassis ID 0015.77c9.7453
 Port ID Type Interface alias
 Port ID port1.0.1
 TTL 120
 Port Description [not configured]
 System Name awplus
 System Description Allied Telesis router/switch, AW+
 v5.4.3A
 System Capabilities - Supported .. Bridge, Router
 - Enabled Bridge, Router
 Management Address 192.168.1.6
 Port VLAN ID (PVID) 1
 Port & Protocol VLAN - Supported . Yes
 - Enabled ... No
 - VIDs 0
 VLAN Names default
 Protocol IDs 9000, 0026424203000000, 888e01, aaaa03,
 88090101, 00540000e302, 0800, 0806, 86dd
 MAC/PHY Auto-negotiation Supported, Enabled
 Advertised Capability 1000BaseTFD, 100BaseTXFD, 100BaseTX,
 10BaseTFD, 10BaseT
 Operational MAU Type 1000BaseTFD (30)
 Power Via MDI (PoE) Supported, Enabled
 Port Class PSE
 Pair Control Ability Disabled
 Power Class Unknown
 Link Aggregation Supported, Disabled
 Maximum Frame Size 1522
 LLDP-MED Device Type Network Connectivity
 LLDP-MED Capabilities LLDP-MED Capabilities, Network Policy,
 Location Identification,
 Extended Power - PSE, Inventory
 Network Policy [not configured]
 Location Identification Civic Address
 Country Code NZ
 City Christchurch
 Street Suffix Avenue
 House Number 27
 Primary Road Name Nazareth
 Location Identification ELIN
 ELIN 123456789012
 Extended Power Via MDI (PoE) PSE
 Power Source Primary Power
 Power Priority Low
 Power Value 4.4 Watts
 Inventory Management:
 Hardware Revision A-0
 Firmware Revision 1.1.0
 Software Revision v5.4.3A
 Serial Number G1Q78900B
 Manufacturer Name Allied Telesis Inc.
 Model Name x610-48Ts/XP
 Asset ID [zero length]

```

Table 41-5: Parameters in the output of **show lldp local-info**

| Parameter                        | Description                                                                                                                 |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------|
| Chassis ID Type                  | Type of the Chassis ID.                                                                                                     |
| Chassis ID                       | Chassis ID that uniquely identifies the local device.                                                                       |
| Port ID Type                     | Type of the Port ID.                                                                                                        |
| Port ID                          | Port ID of the local port through which advertisements are sent.                                                            |
| TTL                              | Number of seconds that the information advertised by the local port remains valid.                                          |
| Port Description                 | Port description of the local port, as specified by the <a href="#">description (interface)</a> command.                    |
| System Name                      | System name, as specified by the <a href="#">hostname</a> command.                                                          |
| System Description               | System description.                                                                                                         |
| System Capabilities (Supported)  | Capabilities that the local port supports.                                                                                  |
| System Capabilities (Enabled)    | Enabled capabilities on the local port.                                                                                     |
| Management Addresses             | Management address associated with the local port. To change this, use the <a href="#">lldp management-address</a> command. |
| Port VLAN ID (PVID)              | VLAN identifier associated with untagged or priority tagged frames received via the local port.                             |
| Port & Protocol VLAN (Supported) | Whether Port & Protocol VLANs (PPV) is supported on the local port.                                                         |
| Port & Protocol VLAN (Enabled)   | Whether the port is in one or more Port & Protocol VLANs.                                                                   |
| Port & Protocol VLAN (VIDs)      | List of identifiers for Port & Protocol VLANs that the port is in.                                                          |
| VLAN Names                       | List of VLAN names for VLANs that the local port is assigned to.                                                            |
| Protocol IDs                     | List of protocols that are accessible through the local port.                                                               |
| MAC/PHY Auto-negotiation         | Auto-negotiation support and current status of the 802.3 LAN on the local port.                                             |



Table 41-5: Parameters in the output of **show lldp local-info** (cont.)

| Parameter                    | Description                                                                                                    |
|------------------------------|----------------------------------------------------------------------------------------------------------------|
| Power Via MDI (PoE)          | PoE-capability and current status on the local port.                                                           |
| Port Class                   | Whether the device is a PSE (Power Sourcing Entity) or a PD (Powered Device)                                   |
| Pair Control Ability         | Whether power pair selection can be controlled                                                                 |
| Power Pairs                  | Which power pairs are selected for power ("Signal Pairs" or "Spare Pairs") if pair selection can be controlled |
| Power Class                  | The power class of the PD device on the port (class 0, 1, 2, 3 or 4)                                           |
| Link Aggregation             | Whether the link is capable of being aggregated and it is currently in an aggregation.                         |
| Aggregated Port-ID           | Aggregated port identifier.                                                                                    |
| Maximum Frame Size           | The maximum frame size capability of the implemented MAC and PHY.                                              |
| LLDP-MED Device Type         | LLDP-MED device type                                                                                           |
| LLDP-MED Capabilities        | Capabilities LLDP-MED capabilities supported on the local port.                                                |
| Network Policy               | List of network policies configured on the local port.                                                         |
| VLAN ID                      | VLAN identifier for the port for the specified application type                                                |
| Tagged Flag                  | Whether the VLAN ID is to be used as tagged or untagged                                                        |
| Layer-2 Priority:            | Layer 2 User Priority (in the range 0 to 7)                                                                    |
| DSCP Value                   | Diffserv codepoint (in the range 0 to 63)                                                                      |
| Location Identification      | Location configured on the local port.                                                                         |
| Extended Power Via MDI (PoE) | PoE-capability and current status of the PoE parameters for Extended Power-Via-MDI TLV on the local port.      |
| Power Source                 | The power source the switch currently uses; either primary power or backup power.                              |
| Power Priority               | The power priority configured on the port; either critical, high or low.                                       |

Table 41-5: Parameters in the output of **show lldp local-info** (cont.)

| Parameter            | Description                                                                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|
| Power Value          | The total power the switch can source over a maximum length cable to a PD device on the port. The value shows the power value in Watts from the PD side. |
| Inventory Management | Inventory information for the device.                                                                                                                    |

**Related  
Commands**

- [description \(interface\)](#)
- [hostname](#)
- [lldp transmit receive](#)

# show lldp neighbors

**Overview** This command displays a summary of information received from neighbors via specified ports. If no port list is supplied, neighbor information for all ports is displayed.

**Syntax** `show lldp neighbors [interface <port-list>]`

| Parameter   | Description                                                  |
|-------------|--------------------------------------------------------------|
| <port-list> | The ports for which the neighbor information is to be shown. |

**Mode** User Exec and Privileged Exec

**Examples** To display neighbor information received via all ports, use the command:

```
awplus# show lldp neighbors
```

To display neighbor information received via ports 1.0.1 and 1.0.6 with LLDP-MED configuration, use the command:

```
awplus# show lldp neighbors interface port1.0.1,port1.0.6
```

**Output** Figure 41-4: Example output from the **show lldp neighbors** command

| LLDP Neighbor Information:                                                      |                     |                  |                         |             |            |
|---------------------------------------------------------------------------------|---------------------|------------------|-------------------------|-------------|------------|
| Total number of neighbors on these ports .... 4                                 |                     |                  |                         |             |            |
| System Capability Codes:                                                        |                     |                  |                         |             |            |
| 0 = Other    P = Repeater    B = Bridge    W = WLAN Access Point                |                     |                  |                         |             |            |
| R = Router   T = Telephone   C = DOCSIS Cable Device   S = Station Only         |                     |                  |                         |             |            |
| LLDP-MED Device Type and Power Source Codes:                                    |                     |                  |                         |             |            |
| 1 = Class I    3 = Class III    PSE = PoE    Both = PoE&Local    Prim = Primary |                     |                  |                         |             |            |
| 2 = Class II   N = Network Con.   Locl = Local   Unkn = Unknown   Back = Backup |                     |                  |                         |             |            |
| Local Port                                                                      | Neighbor Chassis ID | Neighbor Port ID | Neighbor Sys Name       | System Cap. | MED Ty Pwr |
| 1.0.1                                                                           | 002d.3044.7ba6      | port1.0.2        | awplus                  | OPBWRCS     |            |
| 1.0.1                                                                           | 0011.3109.e5c6      | port1.0.3        | AT-9924 switch/route... | --B-R--     |            |
| 1.0.6                                                                           | 0000.10cf.8590      | port3            | AR-442S                 | --B-R--     |            |
| 1.0.6                                                                           | 00ee.4352.df51      | 192.168.1.2      | Jim's desk phone        | --B--T--    | 3 PSE      |

Table 41-6: Parameters in the output of the **show lldp neighbors** command

| Parameter           | Description                                                |
|---------------------|------------------------------------------------------------|
| Local Port          | Local port on which the neighbor information was received. |
| Neighbor Chassis ID | Chassis ID that uniquely identifies the neighbor.          |

Table 41-6: Parameters in the output of the **show lldp neighbors** command

| Parameter           | Description                                                      |
|---------------------|------------------------------------------------------------------|
| Neighbor Port Name  | Port ID of the neighbor.                                         |
| Neighbor Sys Name   | System name of the LLDP neighbor.                                |
| Neighbor Capability | Capabilities that are supported and enabled on the neighbor.     |
| System Capability   | System Capabilities of the LLDP neighbor.                        |
| MED Device Type     | LLDP-MED Device class (Class I, II, III or Network Connectivity) |
| MED Power Source    | LLDP-MED Power Source                                            |

**Related Commands** [show lldp neighbors detail](#)

# show lldp neighbors detail

**Overview** This command displays in detail the information received from neighbors via specified ports. If no port list is supplied, detailed neighbor information for all ports is displayed.

**Syntax** `show lldp neighbors detail [base] [dot1] [dot3] [med] [interface <port-list>]`

| Parameter   | Description                                                  |
|-------------|--------------------------------------------------------------|
| base        | Information for base TLVs.                                   |
| dot1        | Information for 802.1 TLVs.                                  |
| dot3        | Information for 803.1 TLVs.                                  |
| med         | Information for LLDP-MED TLVs.                               |
| <port-list> | The ports for which the neighbor information is to be shown. |

**Mode** User Exec and Privileged Exec

**Examples** To display detailed neighbor information received via all ports, use the command:

```
awplus# show lldp neighbors detail
```

To display detailed neighbor information received via ports 1.0.1, use the command:

```
awplus# show lldp neighbors detail interface port1.0.1
```

**Output** Figure 41-5: Example output from the **show lldp neighbors detail** command

```
awplus# show lldp neighbors detail interface port1.0.1
LLDP Detailed Neighbor Information:

Local port1.0.1:
 Neighbors table last updated 0 hrs 0 mins 40 secs ago

Chassis ID Type MAC address
Chassis ID 0004.cd28.8754
Port ID Type Interface alias
Port ID port1.0.6
TTL 120 (secs)
Port Description [zero length]
System Name awplus
System Description Allied Telesis router/switch, AW+ v5.4.3A
System Capabilities - Supported .. Bridge, Router
 - Enabled Bridge, Router
Management Addresses 0004.cd28.8754
Port VLAN ID (PVID) 1
Port & Protocol VLAN - Supported . Yes
 - Enabled ... Yes
 - VIDs 5
VLAN Names default, vlan5
Protocol IDs 9000, 0026424203000000, 888e01, 8100,
 88090101, 00540000e302, 0800, 0806, 86dd
MAC/PHY Auto-negotiation Supported, Enabled
 Advertised Capability 1000BaseTFD, 100BaseTXFD, 100BaseTX,
 10BaseTFD, 10BaseT
 Operational MAU Type 1000BaseTFD (30)
Power Via MDI (PoE) [not advertised]
Link Aggregation Supported, Disabled
Maximum Frame Size 1522 (Octets)
LLDP-MED Device Type Network Connectivity
LLDP-MED Capabilities LLDP-MED Capabilities, Network Policy,
 Location Identification,
 Extended Power - PSE, Inventory
Network Policy [not advertised]
Location Identification [not advertised]
Extended Power Via MDI (PoE) PD
 Power Source PSE
 Power Priority High
 Power Value 4.4 Watts
Inventory Management:
 Hardware Revision X1-0
 Firmware Revision 1.1.0
 Software Revision v5.4.3A
 Serial Number M1NB73008
 Manufacturer Name Allied Telesis Inc.
 Model Name SBx908
 Asset ID [zero length]
```

Table 41-7: Parameters in the output of the **show lldp neighbors detail** command

| Parameter                        | Description                                                                               |
|----------------------------------|-------------------------------------------------------------------------------------------|
| Chassis ID Type                  | Type of the Chassis ID.                                                                   |
| Chassis ID                       | Chassis ID that uniquely identifies the neighbor.                                         |
| Port ID Type                     | Type of the Port ID.                                                                      |
| Port ID                          | Port ID of the neighbor.                                                                  |
| TTL                              | Number of seconds that the information advertised by the neighbor remains valid.          |
| Port Description                 | Port description of the neighbor's port.                                                  |
| System Name                      | Neighbor's system name.                                                                   |
| System Description               | Neighbor's system description.                                                            |
| System Capabilities (Supported)  | Capabilities that the neighbor supports.                                                  |
| System Capabilities (Enabled)    | Capabilities that are enabled on the neighbor.                                            |
| Management Addresses             | List of neighbor's management addresses.                                                  |
| Port VLAN ID (PVID)              | VLAN identifier associated with untagged or priority tagged frames for the neighbor port. |
| Port & Protocol VLAN (Supported) | Whether Port & Protocol VLAN is supported on the LLDP neighbor.                           |
| Port & Protocol VLAN (Enabled)   | Whether Port & Protocol VLAN is enabled on the LLDP neighbor.                             |
| Port & Protocol VLAN (VIDs)      | List of Port & Protocol VLAN identifiers.                                                 |
| VLAN Names                       | List of names of VLANs that the neighbor's port belongs to.                               |
| Protocol IDs                     | List of protocols that are accessible through the neighbor's port.                        |
| MAC/PHY Auto-negotiation         | Auto-negotiation configuration and status                                                 |
| Power Via MDI (PoE)              | PoE configuration and status of 802.3 Power-Via-MDI TLV                                   |
| Link Aggregation                 | Link aggregation information                                                              |
| Maximum Frame Size               | The maximum frame size capability                                                         |

Table 41-7: Parameters in the output of the **show lldp neighbors detail** command (cont.)

| Parameter                    | Description                       |
|------------------------------|-----------------------------------|
| LLDP-MED Device Type         | LLDP-MED Device type              |
| LLDP-MED Capabilities        | LLDP-MED capabilities supported   |
| Network Policy               | List of network policies          |
| Location Identification      | Location information              |
| Extended Power Via MDI (PoE) | PoE-capability and current status |
| Inventory Management         | Inventory information             |

**Related  
Commands** [show lldp neighbors](#)



# show lldp statistics

**Overview** This command displays the global LLDP statistics (packet and event counters).

**Syntax** show lldp statistics

**Mode** User Exec and Privileged Exec

**Example** To display global LLDP statistics information, use the command:

```
awplus# show lldp statistics
```

## Output

Table 41-8: Example output from the **show lldp statistics** command

```
awplus# show lldp statistics

Global LLDP Packet and Event counters:

Frames: Out 345
 In 423
 In Errored 0
 In Dropped 0
TLVs: Unrecognized 0
 Discarded 0
Neighbors: New Entries 20
 Deleted Entries 20
 Dropped Entries 0
 Entry Age-outs 20
```

Table 41-9: Parameters in the output of the **show lldp statistics** command

| Parameter                 | Description                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------------------|
| Frames Out                | Number of LLDPDU frames transmitted.                                                                         |
| Frames In                 | Number of LLDPDU frames received.                                                                            |
| Frames In Errored         | Number of invalid LLDPDU frames received.                                                                    |
| Frames In Dropped         | Number of LLDPDU frames received and discarded for any reason.                                               |
| TLVs Unrecognized         | Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types. |
| TLVs Discarded            | Number of LLDP TLVs discarded for any reason.                                                                |
| Neighbors New Entries     | Number of times the information advertised by neighbors has been inserted into the neighbor table.           |
| Neighbors Deleted Entries | Number of times the information advertised by neighbors has been removed from the neighbor table.            |

Table 41-9: Parameters in the output of the **show lldp statistics** command (cont.)

| Parameter                           | Description                                                                                                                                        |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Neighbors<br>Dropped Entries        | Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.            |
| Neighbors Entry<br>Age-outs Entries | Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired. |

**Related  
Commands**

[clear lldp statistics](#)

[show lldp statistics interface](#)

# show lldp statistics interface

**Overview** This command displays the LLDP statistics (packet and event counters) for specified ports. If no port list is supplied, LLDP statistics for all ports are displayed.

**Syntax** `show lldp statistics interface [<port-list>]`

| Parameter                      | Description                                         |
|--------------------------------|-----------------------------------------------------|
| <code>&lt;port-list&gt;</code> | The ports for which the statistics are to be shown. |

**Mode** User Exec and Privileged Exec

**Examples** To display LLDP statistics information for all ports, use the command:

```
awplus# show lldp statistics interface
```

To display LLDP statistics information for ports 1.0.1 and 1.0.6, use the command:

```
awplus# show lldp statistics interface port1.0.1,port1.0.6
```

## Output

Table 41-10: Example output from the **show lldp statistics interface** command

```
awplus# show lldp statistics interface port1.0.1,port1.0.6

LLDP Packet and Event Counters:

port1.0.1
 Frames: Out 27
 In 22
 In Errored 0
 In Dropped 0
 TLVs: Unrecognized 0
 Discarded 0
 Neighbors: New Entries 3
 Deleted Entries 0
 Dropped Entries 0
 Entry Age-outs 0

port1.0.6
 Frames: Out 15
 In 18
 In Errored 0
 In Dropped 0
 TLVs: Unrecognized 0
 Discarded 0
 Neighbors: New Entries 1
 Deleted Entries 0
 Dropped Entries 0
 Entry Age-outs 0
```

Table 41-11: Parameters in the output of the **show lldp statistics interface** command

| Parameter                 | Description                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------------------|
| Frames Out                | Number of LLDPDU frames transmitted.                                                                         |
| Frames In                 | Number of LLDPDU frames received.                                                                            |
| Frames In Errored         | Number of invalid LLDPDU frames received.                                                                    |
| Frames In Dropped         | Number of LLDPDU frames received and discarded for any reason.                                               |
| TLVs Unrecognized         | Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types. |
| TLVs Discarded            | Number of LLDP TLVs discarded for any reason.                                                                |
| Neighbors New Entries     | Number of times the information advertised by neighbors has been inserted into the neighbor table.           |
| Neighbors Deleted Entries | Number of times the information advertised by neighbors has been removed from the neighbor table.            |

Table 41-11: Parameters in the output of the **show lldp statistics interface** command (cont.)

| Parameter                        | Description                                                                                                                                        |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Neighbors Dropped Entries        | Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.            |
| Neighbors Entry Age-outs Entries | Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired. |

**Related  
Commands**   [clear lldp statistics](#)  
[show lldp statistics](#)

# show location

**Overview** Use this command to display selected location information configured on the switch.

**Syntax** show location {civic-location|coord-location|elin-location}  
show location {civic-location|coord-location|elin-location}  
identifier {<civic-loc-id>|<coord-loc-id>|<elin-loc-id>}  
show location {civic-location|coord-location|elin-location}  
interface <port-list>

| Parameter      | Description                                                |
|----------------|------------------------------------------------------------|
| civic-location | Display civic location information.                        |
| coord-location | Display coordinate location information.                   |
| elin-location  | Display ELIN location information.                         |
| <civic-loc-id> | Civic address location identifier, in the range 1 to 4095. |
| <coord-loc-id> | Coordinate location identifier, in the range 1 to 4095.    |
| <elin-loc-id>  | ELIN location identifier, in the range 1 to 4095.          |
| <port-list>    | Ports to display information about.                        |

**Mode** User Exec and Privileged Exec

**Examples** To display a civic address location configured on port1.0.1, use the command:  
awplus# show location civic-location interface port1.0.1

Table 41-12: Example output from the **show location** command

| awplus# show location civic-location interface port1.0.1 |    |                   |              |       |
|----------------------------------------------------------|----|-------------------|--------------|-------|
| Port                                                     | ID | Element Type      | Element      | Value |
| -----                                                    |    |                   |              |       |
| 1.0.1                                                    | 1  | Country           | NZ           |       |
|                                                          |    | City              | Christchurch |       |
|                                                          |    | Street-suffix     | Avenue       |       |
|                                                          |    | House-number      | 27           |       |
|                                                          |    | Primary-road-name | Nazareth     |       |

To display coordinate location information configured on the identifier 1, use the command:

```
awplus# show location coord-location identifier 1
```

Table 41-13: Example output from the **show location** command

| awplus# show location coord-location identifier 1 |           |            |                                       |
|---------------------------------------------------|-----------|------------|---------------------------------------|
| ID                                                | Element   | Type       | Element Value                         |
| -----                                             |           |            |                                       |
| 1                                                 | Latitude  | Resolution | 15 bits                               |
|                                                   | Latitude  |            | 38.8986481130123138427734375 degrees  |
|                                                   | Longitude | Resolution | 15 bits                               |
|                                                   | Longitude |            | 130.2323232293128967285156250 degrees |
|                                                   | Altitude  | Resolution | 10 bits                               |
|                                                   | Altitude  |            | 2.50000000 meters                     |
|                                                   | Map       | Datum      | WGS 84                                |

The coordinate location information displayed may differ from the information entered because it is stored in binary format. For more information, see the [location coord-location configuration](#) command.

To display all ELIN location information configured on the switch, use the command:

```
awplus# show location elin-location
```

Table 41-14: Example output from the **show location elin-location** command

| awplus# show location elin-location |            |
|-------------------------------------|------------|
| ID                                  | ELIN       |
| -----                               |            |
| 1                                   | 1234567890 |
| 2                                   | 5432154321 |

### Related Commands

[location elin-location-id](#)  
[location civic-location identifier](#)  
[location civic-location configuration](#)  
[location coord-location identifier](#)  
[location coord-location configuration](#)  
[location elin-location](#)

# 42

# SMTP Commands

## Introduction

**Overview** This chapter provides an alphabetical reference for commands used to configure SMTP.

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](#).

- Command List**
- [“debug mail”](#) on page 1393
  - [“delete mail”](#) on page 1394
  - [“mail”](#) on page 1395
  - [“mail from”](#) on page 1396
  - [“mail smtpserver”](#) on page 1397
  - [“show counter mail”](#) on page 1398
  - [“show mail”](#) on page 1399
  - [“undebbug mail”](#) on page 1400



# 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 mail  
show counter mail  
undebug mail

# delete mail

**Overview** This command deletes mail from the queue.

**Syntax** delete mail [mail-id <mail-id>|all]

| Parameter | Description                                                                                                        |
|-----------|--------------------------------------------------------------------------------------------------------------------|
| mail-id   | Deletes a single mail from the mail queue.                                                                         |
|           | <mail-id> An 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 a 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

**Example** To send an email to rei@nerv.com with the subject dummy plug configuration, and with the message body inserted from the file plug.conf use the command:

```
awplus# mail rei@nerv.com subject dummy plug configuration
filename plug.conf
```

**Related Commands**

- [debug mail](#)
- [delete mail](#)
- [mail from](#)
- [mail smtpserver](#)
- [show mail](#)
- [show counter mail](#)

# mail from

**Overview** This command sets an email address for the “mail from” SMTP command. You must specify a sending email address with this command before you can send any email.

**Syntax** mail from <from>

| Parameter | Description                                   |
|-----------|-----------------------------------------------|
| <from>    | The email address that the mail is sent from. |

**Mode** Global Configuration

**Example** To set the email address from which you are sending mail to “kaji@nerv.com”, use the command:

```
awplus(config)# mail from kaji@nerv.com
```

**Related Commands**

- [delete mail](#)
- [mail](#)
- [mail smtpserver](#)
- [show mail](#)

# mail smtpserver

**Overview** This command sets the IP address of the SMTP server that your device sends email to. You must specify a mail server with this command before you can send any email.

**Syntax** mail smtpserver *<ip-address>*

| Parameter                 | Description                                                   |
|---------------------------|---------------------------------------------------------------|
| <i>&lt;ip-address&gt;</i> | Internet Protocol (IP) Address for the mail server specified. |

**Mode** Global Configuration

**Example** To specify a mail server at 192.168.0.1, use the command:

```
awplus# mail smtpserver 192.168.0.1
```

**Related Commands**

- debug mail
- delete mail
- mail
- mail from
- show mail
- show counter mail

# show counter mail

**Overview** This command displays the mail counters.

**Syntax** show counter mail

**Mode** User Exec and Privileged Exec

**Output** Figure 42-1: Example output from the **show counter mail** command

```
Mail Client (SMTP) counters
Mails Sent 0
Mails Sent Fails 1
```

Table 42-1: 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. |

**Example** To show the emails in the queue use the command:

```
awplus# show counter mail
```

**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
```

**Related  
Commands**

- [delete mail](#)
- [mail](#)
- [show counter mail](#)

# undebbug mail

**Overview** This command applies the functionality of the no [debug mail](#) command.



# 43

# 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Command List**
- [“rmon alarm”](#) on page 1402
  - [“rmon collection history”](#) on page 1404
  - [“rmon collection stats”](#) on page 1405
  - [“rmon event”](#) on page 1406
  - [“show rmon alarm”](#) on page 1407
  - [“show rmon event”](#) on page 1408
  - [“show rmon history”](#) on page 1410
  - [“show rmon statistics”](#) on page 1412

# 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:** Only alarms for switch port interfaces, not for VLAN interfaces, can be configured.

**Syntax** `rmon alarm <alarm-index> <oid> 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>]`  
`no rmon alarm <alarm-index>`

| Parameter                       | Description                                                                                                                                                                                                                                                                                                                           |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <alarm-index>                   | <1-65535> Alarm entry index value.                                                                                                                                                                                                                                                                                                    |
| <oid>                           | The variable SNMP MIB Object Identifier (OID) name to be monitored, in the format etherStatsEntry.field.<stats-index>. For example, etherStatsEntry.5.22 is the OID for the etherStatsPkts field in the etherStatsEntry table for the interface defined by the <stats-index> 22 in the <a href="#">rmon collection stats</a> command. |
| interval<1-2147483647>          | Polling interval in seconds.                                                                                                                                                                                                                                                                                                          |
| 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.                                                                                                                                                                                                                                                                  |
| rising-threshold<1-2147483647>  | Rising threshold value of the alarm entry in seconds.                                                                                                                                                                                                                                                                                 |
| <rising-event-index>            | <1-65535> The event to be triggered when the monitored object value reaches the rising threshold value. This is an event index of an event specified by the <a href="#">rmon event</a> command.                                                                                                                                       |
| falling-threshold<1-2147483647> | Falling threshold value of the alarm entry in seconds.                                                                                                                                                                                                                                                                                |
| <falling-event-index>           | <1-65535> 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.                                                                                                                                      |

| Parameter            | Description                                                                                                                                                 |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. |
| owner <owner>        | Arbitrary owner name to identify the alarm entry.                                                                                                           |

**Default** By default, there are no alarms.

**Mode** Global Configuration

**Usage** 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 the SNMP MIB Object Identifier (OID) indicated in the command syntax with < **oid** > must be specified as a dotted decimal value with the form **etherStatsEntry.field.<stats-index>**.

**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), to trigger event 2 (defined by the [rmon event](#) command) when it reaches the rising threshold 400, and to trigger event 3 when it reaches the falling threshold 200, and identify this alarm as belonging to Maria, use the 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
```

**Related  
Commands** [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:** Only a history for switch port interfaces, not for VLAN interfaces, can be collected.

**Syntax** `rmon collection history <history-index> [buckets <1-65535>]  
[interval <1-3600>] [owner <owner>]  
no rmon collection history <history-index>`

| Parameter         | Description                                                         |
|-------------------|---------------------------------------------------------------------|
| <history-index>   | <1-65535> A unique RMON history control entry index value.          |
| buckets <1-65535> | Number of requested buckets to store snapshots. Default 50 buckets. |
| interval <1-3600> | Polling interval in seconds. Default 1800 second polling interval.  |
| owner<owner>      | Owner name to identify the entry.                                   |

**Default** The default interval is 1800 seconds and the default buckets is 50 buckets.

**Mode** Interface Configuration

**Example** To create a history statistics control group to store 200 snapshots with an interval of 500 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
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)# interface port1.0.2
awplus(config-if)# no rmon collection history 200
```

## 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:** Only statistics for switch port interfaces, not for VLAN interfaces, can be collected.

**Syntax** `rmon collection stats <collection-index> [owner <owner>]`  
`no rmon collection stats <collection-index>`

| Parameter          | Description                                                                                                                                                             |
|--------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <collection-index> | <1-65535> 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. |
| 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)# interface port1.0.2
awplus(config-if)# rmon collection stats 200 owner myrtle
```

To to stop collecting RMON statistics, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no rmon collection stats 200
```

## rmon event

**Overview** Use this command to create an event definition for a log or a trap or both. The event index for this event can then be referred to by the [rmon alarm](#) command.

Use the **no** variant of this command to remove the event definition.

**NOTE:** Only the events for switch port interfaces, not for VLAN interfaces, can be collected.

**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 for a log with an index of 299, use this command:

```
awplus# configure terminal
awplus(config)# rmon event 299 log description cond3 owner
alfred
```

To 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.

**NOTE:** *Only the alarms for switch port interfaces, not for VLAN interfaces, can be shown.*

**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.

**NOTE:** Only the events for switch port interfaces, not for VLAN interfaces, can be shown.

**Syntax** show rmon event

**Mode** User Exec and Privileged Exec

**Output** Figure 43-1: 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.

**NOTE:** Only the history for switch port interfaces, not for VLAN interfaces, can be shown.

**Syntax** show rmon history

**Mode** User Exec and Privileged Exec

**Output** Figure 43-2: 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.

**NOTE:** Only statistics for switch port interfaces, not for VLAN interfaces, can be shown.

**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 43-3: 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](#)

# 44

# 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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

- Command List**
- [“active \(trigger\)”](#) on page 1416
  - [“day”](#) on page 1417
  - [“debug trigger”](#) on page 1419
  - [“description \(trigger\)”](#) on page 1420
  - [“repeat”](#) on page 1421
  - [“script”](#) on page 1422
  - [“show debugging trigger”](#) on page 1424
  - [“show running-config trigger”](#) on page 1425
  - [“show trigger”](#) on page 1426
  - [“test”](#) on page 1431
  - [“time \(trigger\)”](#) on page 1432
  - [“trap”](#) on page 1434
  - [“trigger”](#) on page 1435
  - [“trigger activate”](#) on page 1436
  - [“type atmf node”](#) on page 1437
  - [“type cpu”](#) on page 1440
  - [“type interface”](#) on page 1441

- [“type memory”](#) on page 1442
- [“type periodic”](#) on page 1443
- [“type ping-poll”](#) on page 1444
- [“type reboot”](#) on page 1445
- [“type time”](#) on page 1446
- [“type usb”](#) on page 1447
- [“undebug trigger”](#) on page 1448

## 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

**Mode** Trigger Configuration

**Usage** 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](#)



# day

**Overview** This command specifies the days or date that the can trigger activate on. You can specify either:

- A specific date
- A specific day of the week
- A list of days of the week
- every day

By default, the trigger can activate on any day.

**Syntax** day every-day  
day <1-31> <month> <2000-2035>  
day <weekday>

| Parameter   | Description                                                                                                                                                                                                                 |
|-------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| every-day   | Sets the trigger so that it can activate on any day.                                                                                                                                                                        |
| <1-31>      | Day of the month the trigger is permitted to activate on.                                                                                                                                                                   |
| <month>     | 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>                               |
| <2000-2035> | Sets the year that the trigger is permitted to activate in.                                                                                                                                                                 |
| <weekday>   | 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> |

**Mode** Trigger Configuration

**Usage** 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 Jun 2010, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 55
awplus(config-trigger)# day 1 Jun 2010
```

To permit trigger 12 to activate on a Mondays, Wednesdays and Fridays, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# day monday wednesday friday
```

**Related  
Commands**   [show trigger](#)  
[trigger](#)

# 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                                          |
|----------------|------------------------------------------------------|
| yes   forever  | The trigger repeats indefinitely, or until disabled. |
| no   once      | The trigger activates only once.                     |
| <1-4294967294> | 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 44-1: 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
```

**Output** Figure 44-2: 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 44-1: Example output from the **show trigger** command

```
awplus#show trigger
```

| TR# | Type & Details       | Name                 | Ac | Te | Tr | Repeat     | #Scr | Days/Date  |
|-----|----------------------|----------------------|----|----|----|------------|------|------------|
| 001 | USB (in)             |                      | Y  | N  | Y  | Continuous | 0    | smtwtfs    |
| 002 | USB (out)            |                      | Y  | N  | Y  | Continuous | 0    | smtwtfs    |
| 003 | CPU (80% any)        | Busy CPU             | Y  | N  | Y  | 5          | 1    | smtwtfs    |
| 005 | Periodic (30 min)    | Regular status check | Y  | N  | N  | Continuous | 1    | -mtwtf-    |
| 007 | Memory (85% up)      | High mem usage       | Y  | N  | Y  | 8          | 1    | smtwtfs    |
| 011 | Time (00:01)         | Weekend access       | Y  | N  | Y  | Continuous | 1    | -----s     |
| 013 | Reboot               |                      | Y  | N  | Y  | Continuous | 2    | smtwtfs    |
| 017 | Interface (vlan1 ... | Change config for... | Y  | N  | Y  | Once       | 1    | 2-apr-2008 |
| 019 | Ping-poll (5 up)     | Connection to svr1   | Y  | N  | Y  | Continuous | 1    | smtwtfs    |

Table 44-2: Parameters in the output of the **show trigger** command

| 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. |

Table 44-2: Parameters in the output of the **show trigger** command (cont.)

| Parameter | Description                                                                                                                                                                                                         |
|-----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ac        | Whether the trigger is active (Y), or inactive (N).                                                                                                                                                                 |
| Te        | Whether the trigger is in test mode (Y) or not (N).                                                                                                                                                                 |
| Tr        | Whether or not the trigger is enabled to send SNMP traps. See the <a href="#">trap</a> command.                                                                                                                     |
| 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 show trigger <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 44-3: Example output from the **show trigger** command for a specific trigger

```
awplus#show trigger 3
Trigger Configuration Details

Trigger 1
Description display cpu usage when pass 80%
Type and details CPU (80% up)
Days 26-nov-2007
After 00:00:00
Before 23:59:59
Active Yes
Test No
Trap Yes
Repeat 123 (0)
Modified Tue Dec 20 02:26:03 1977
Number of activations 0
Last activation not activated
Number of scripts 1
 1. shocpu.scp
 2. <not configured>
 3. <not configured>
 4. <not configured>
 5. <not configured>

```

To display detailed information about all triggers, use the command:

```
awplus# show trigger full
```

Table 44-3: Example output from the **show trigger full** command

```
awplus#show trigger full
Trigger Configuration Details

Trigger 1
Description <no description>
Type and
details USB (in)
Days smtwtfS
After 00:00:00
Before 23:59:59
Active Yes
Test No
Trap Yes
Repeat Continuous
Modified Fri Sep 3 14:45:56 2010
Number of activations 0
Last activation not activated
Number of scripts 0
 1. <not configured>
 2. <not configured>
 3. <not configured>
 4. <not configured>
 5. <not configured>

Trigger 2
Description <no description>
Type and
details USB (out)
Days smtwtfS
After 00:00:00
Before 23:59:59
Active Yes
Test No
Trap Yes
Repeat Continuous
Modified Fri Sep 3 14:45:56 2010
Number of activations 0
Last activation not activated
Number of scripts 0
 1. <not configured>
 2. <not configured>
 3. <not configured>
 4. <not configured>
 5. <not configured>
```

Table 44-4: Parameters in the output of the **show trigger full** and **show trigger** commands for a specific trigger

| Parameter   | Description                      |
|-------------|----------------------------------|
| Trigger     | The ID of the trigger.           |
| Description | Descriptive name of the trigger. |

Table 44-4: Parameters in the output of the **show trigger full** and **show trigger** commands for a specific trigger (cont.)

| Parameter             | Description                                                                                                                                                                                                                                   |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Type and details      | The trigger type and its activation conditions.                                                                                                                                                                                               |
| Days                  | The days on which the trigger is permitted to activate.                                                                                                                                                                                       |
| 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 44-4: Example output from the **show trigger counter** command

```
awplus#show trigger counter
Trigger Module Counters

Trigger activations 0
Time triggers activated today 0
Periodic triggers activated today 0
Interface triggers activated today 0
Resource triggers activated today 0
Reboot triggers activated today 0
Ping-poll triggers activated today 0

```

Table 44-5: Parameters in the output of the **show trigger counter** command

| Parameter                          | Description                                                                |
|------------------------------------|----------------------------------------------------------------------------|
| Trigger activations                | Number of times a trigger has been activated.                              |
| Time triggers activated today      | Number of times a time trigger has been activated today.                   |
| Periodic triggers activated today  | Number of times a periodic trigger has been activated today.               |
| Interface triggers activated today | Number of times an interface trigger has been activated today.             |
| Resource triggers activated today  | Number of times a CPU or memory resource trigger has been activated today. |
| Ping-poll triggers activated today | Number of times a ping-poll trigger has been activated today.              |

**Related** [trigger](#)  
**Commands**

# 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** 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:

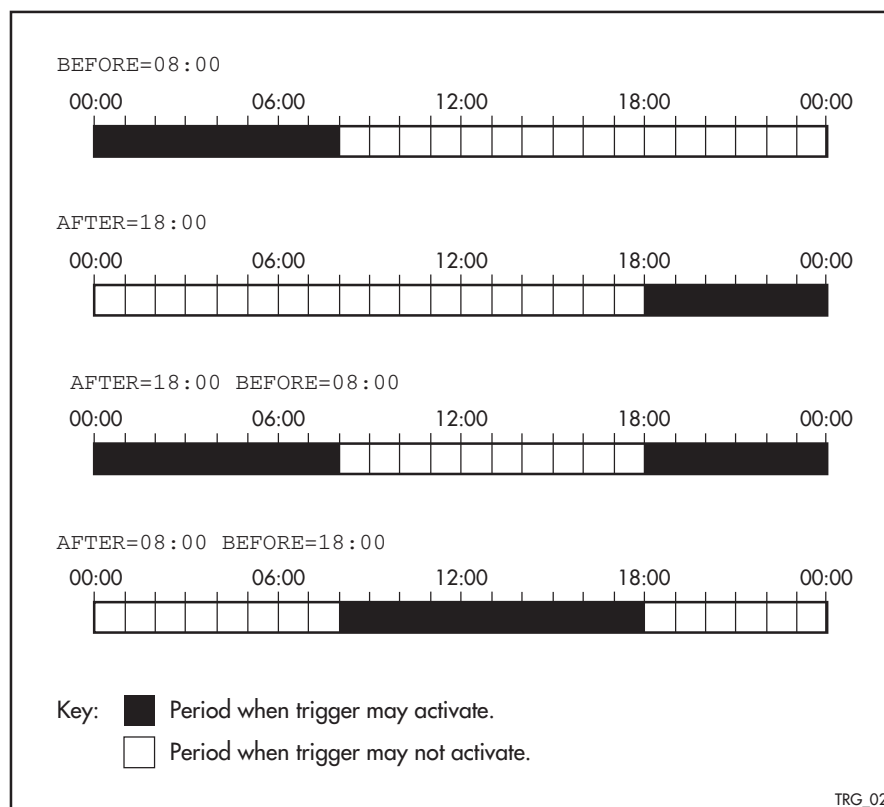
```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no test
```

**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** 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** You must configure SNMP before using traps with triggers. For more information, see:

- the [SNMP MIBs Overview](#), for information about which MIB objects are supported.
- the [SNMP Feature Overview and Configuration Guide](#).

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 [SNMP MIBs Overview](#) 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 command:

```
awplus# trigger 12
```

To completely remove all configuration associated with trigger 12, use the command:

```
awplus# 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** This command manually activates a trigger without the normal trigger conditions being met.

The trigger is activated even if it is configured as inactive. 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** [show trigger](#)  
[trigger](#)

## type atmf node

**Overview** This command configures a trigger to be activated at an AMF node join event or leave event.

**Syntax** type atmf node {join|leave}

| Parameter | Description           |
|-----------|-----------------------|
| join      | AMF node join event.  |
| leave     | AMF node leave event. |

**Mode** Trigger Configuration

**CAUTION:** *Only configure this trigger on one device because it is a network wide event.*

**Example 1** To configure trigger 5 to activate at an AMF node leave event, 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 smtwtf
005 ATMF node (leave) E-mail on ATMF Exit Y N Y Continuous 1 smtwtf

=====
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 smtwtf

```

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** 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. This can be the name of a device port, an eth-management port, or a VLAN. |
| 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 port1.0.2 becomes operational, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 19
awplus(config-trigger)# type interface port1.0.2 up
```

**Related  
Commands** [show trigger](#)  
[trigger](#)

# 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** 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                       |
|-----------|-----------------------------------|
| <hh:mm>   | 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](#)

# type usb

**Overview** Use this command to configure a trigger that activates on either the removal or the insertion of a USB storage device.

**Syntax** type usb {in|out}

| Parameter | Description                                             |
|-----------|---------------------------------------------------------|
| in        | Trigger activates on insertion of a USB storage device. |
| out       | Trigger activates on removal of a USB storage device.   |

**Mode** Trigger Configuration

**Usage** USB triggers cannot execute script files from a USB storage device.  
For example trigger configurations that use the **type usb** command, see “Capture Show Output and Save to a USB Storage Device” in the [Triggers Feature Overview and Configuration Guide](#).

**Examples** To configure trigger 1 to activate on the insertion of a USB storage device, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 1
awplus(config-trigger)# type usb in
```

**Related Commands** [trigger](#)  
[show running-config trigger](#)  
[show trigger](#)

# undebug trigger

**Overview** This command applies the functionality of the **no debug trigger** command.



# 45

# Ping-Polling Commands

## Introduction

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 “Controlling “show” Command Output” in the [“Getting Started with AlliedWare Plus” Feature Overview and Configuration Guide](#).

Table 45-1: 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 1451
  - [“clear ping-poll”](#) on page 1452
  - [“critical-interval”](#) on page 1453
  - [“debug ping-poll”](#) on page 1454

- [“description \(ping-polling\)”](#) on page 1455
- [“fail-count”](#) on page 1456
- [“ip \(ping-polling\)”](#) on page 1457
- [“length \(ping-poll data\)”](#) on page 1458
- [“normal-interval”](#) on page 1459
- [“ping-poll”](#) on page 1460
- [“sample-size”](#) on page 1461
- [“show counter ping-poll”](#) on page 1463
- [“show ping-poll”](#) on page 1466
- [“source-ip”](#) on page 1471
- [“timeout \(ping polling\)”](#) on page 1472
- [“up-count”](#) on page 1473
- [“undebg ping-poll”](#) on page 1474

## 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                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------|
| <code>&lt;1-65536&gt;</code> | 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                                                                                                                        |
|-----------|------------------------------------------------------------------------------------------------------------------------------------|
| <1-100>   | 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                                                                 |
|-----------|-----------------------------------------------------------------------------|
| <4-1500>  | 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                                                 |
|-----------|-------------------------------------------------------------|
| <1-65536> | 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                   |
|-----------|-------------------------------|
| <1-100>   | 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                                             |
|----------------------------|---------------------------------------------------------|
| <code>&lt;1-100&gt;</code> | 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 45-1: 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 45-2: 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.                                                                                                               |



Table 45-2: Parameters in output of the **show counter ping-poll** command

| Parameter        | Description                                                                                        |
|------------------|----------------------------------------------------------------------------------------------------|
| 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 45-2: 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 45-3: 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 45-3: 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 45-3: 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 45-4: 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.                   |

Table 45-4: Parameters in output of the **show ping-poll** command (cont.)

| Parameter         | Description                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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.                                                                                                                                  |
| 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 6 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                                                                      |
|-----------|----------------------------------------------------------------------------------|
| <1-100>   | 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.