AMF Plus Cloud

AUTONOMOUS MANAGEMENT FRAMEWORK PLUS (AMF PLUS) FOR CLOUD-BASED NETWORK MANAGEMENT

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

C613-50715-01 Rev A

Acknowledgments

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

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

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

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

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

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

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

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

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

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

© 2025 Allied Telesis, Inc.

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

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

Contents

PART 1: Setup and Troubleshooting 42

Chapter 1: CLI Navigation Commands 43

Introduction 43
configure terminal 44
disable (Privileged Exec mode) 45
do 46
enable (Privileged Exec mode) 47
end 49
exit 50
help 51
logout 52
show history 53

Chapter 2: Vista Manager EX Commands 54

Introduction 54
atmf topology-gui enable 55
http log webapi-requests 56
http port 57
http secure-port 58
http trustpoint 59
log event-host 61
service http 62
show http 63

Chapter 3: File and Configuration Management Commands 64

Introduction 64
boot config-file 67
boot config-file backup 68
cd 69
copy (filename) 70
copy debug 72
copy running-config 73

copy startup-config 74
copy zmodem 75
delete 76
delete debug 77
dir 78
edit 80
erase factory-default 81
erase startup-config 82
ip tftp source-interface 83
ipv6 tftp source-interface 84
mkdir 85
move 86
move debug 87
pwd 88
rmdir 89
show boot 90
show hash 91
show file 92
show file systems 93
show running-config 95
show running-config interface 98
show running-config unencrypted 100
show startup-config 101
show version 102
software-upgrade 103
strict-user-process-control 104
strict-user-process-control force 105
write file 106
write memory 107
write terminal 108

Chapter 4: User Access Commands 109

Introduction 109
aaa authentication enable default local 111
aaa local authentication attempts lockout-time 112
aaa local authentication attempts max-fail 113
aaa login fail-delay 114
clear aaa local user lockout 115
clear line vty 116
enable password 117
enable secret (deprecated) 119
exec-timeout 120
length (asyn) 121
line 122
privilege level 123
security-password history 124
security-password forced-change 125
security-password lifetime 126
security-password min-lifetime-enforce 127
security-password minimum-categories 128
security-password minimum-length 129
security-password reject-expired-pwd 130
security-password warning 131

service advanced-vty 132
service password-encryption 133
service telnet 134
show aaa local user locked 135
show privilege 137
show security-password configuration 138
show security-password user 139
show telnet 140
show users 141
strict-user-process-control 142
strict-user-process-control force 143
telnet 144
telnet server 145
terminal length 146
terminal resize 147
username 148

Chapter 5: Subscription Licensing Commands 150
Introduction 150
license update file 151
license update online 152
show license external 153

Chapter 6: System Configuration and Monitoring Commands 154
Introduction 154
banner display external-manager 156
banner exec 157
banner external-manager 159
banner login (system) 161
banner motd 163
clock set 165
clock summer-time date 166
clock summer-time recurring 168
clock timezone 170
hostname 171
low-memory restart 172
no debug all 173
reboot 175
reload 176
show banner external-manager 177
show clock 178
show cpu 180
show cpu history 183
show debugging 185
show interface memory 186
show memory 188
show memory allocations 190
show memory history 192
show memory pools 193
show memory shared 194
show process 195
show reboot history 197

show router-id 198
show system 199
show system mac 200
show system serialnumber 201
show tech-support 202
terminal monitor 204
undebug all 205

Chapter 7: Logging Commands 206
Introduction 206
clear exception log 208
clear log 209
clear log buffered 210
clear log permanent 211
copy buffered-log 212
copy permanent-log 213
default log buffered 214
default log console 215
default log email 216
default log host 217
default log monitor 218
default log permanent 219
log buffered 220
log buffered (filter) 221
log buffered exclude 224
log buffered size 227
log console 228
log console (filter) 229
log console exclude 232
log email 235
log email (filter) 236
log email exclude 239
log email time 242
log facility 244
log host 246
log host (filter) 248
log host exclude 251
log host source 254
log host startup-delay 255
log host time 257
log monitor (filter) 259
log monitor exclude 262
log permanent 265
log permanent (filter) 266
log permanent exclude 269
log permanent size 272
log-rate-limit nsm 273
log trustpoint 274
show counter log 275
show exception log 276
show log 277
show log config 279
show log permanent 281

show running-config log 283

Chapter 8: Scripting Commands 284
Introduction 284
activate 285
echo 286
wait 287

Chapter 9: Interface Commands 288
Introduction 288
description (interface) 289
interface (to configure) 290
mtu 292
service statistics interfaces counter 294
show interface 295
show interface brief 298
show interface memory 299
show interface status 301
shutdown 303

PART 2: Interfaces and Layer 2 304

Chapter 10: Bridging Commands 305
Introduction 305
ageing-time 306
bridge 307
bridge-group 308
l3-filtering enable 310
mac-learning 311
show bridge 312
show bridge macaddr 314

Chapter 11: 802.1Q Encapsulation Commands 315
Introduction 315
encapsulation dot1q 316

PART 3: Layer 3 Switching 318

Chapter 12: IP Addressing and Protocol Commands 319
Introduction 319
arp 321
arp log 322
arp opportunistic-nd 325
arp-loose-check 326
clear arp-cache 327
debug ip packet interface 328
ip address (IP Addressing and Protocol) 330
ip forwarding 332
ip icmp error-interval 333
ip icmp-timestamp 334
ip tcp synack-retries 335

ip tcp-timestamp 336
ip unreachables 337
ping 339
show arp 340
show ip flooding-nexthops 341
show ip forwarding 342
show ip interface 343
show ip sockets 344
tcpdump 347
traceroute 348
undebug ip packet interface 349

Chapter 13: Domain Name Service (DNS) Commands 350
Introduction 350
ip dns forwarding domain-list 351
ip domain-list 352
ip domain-lookup 353
ip domain-name 354
ip name-server 355
show hosts 357
show ip domain-list 358
show ip domain-name 359
show ip name-server 360

Chapter 14: IPv6 Commands 361
Introduction 361
clear ipv6 neighbors 363
ipv6 address 364
ipv6 address autoconfig 365
ipv6 address suffix 367
ipv6 enable 368
ipv6 eui64-linklocal 370
ipv6 forwarding 371
ipv6 icmp error-interval 372
ipv6 nd accept-ra-default-routes 373
ipv6 nd accept-ra-pinfo 374
ipv6 nd current-hoplimit 375
ipv6 nd dns search-list 376
ipv6 nd dns-server 377
ipv6 nd managed-config-flag 378
ipv6 nd minimum-ra-interval 379
ipv6 nd other-config-flag 380
ipv6 nd prefix 381
ipv6 nd ra-interval 383
ipv6 nd ra-lifetime 384
ipv6 nd reachable-time 385
ipv6 nd retransmission-time 386
ipv6 nd route-information 387
ipv6 nd router-preference 388
ipv6 nd suppress-ra 389
ipv6 opportunistic-nd 390
ipv6 route 391

ipv6 unreachables 393
ping ipv6 394
show ipv6 forwarding 396
show ipv6 interface 397
show ipv6 neighbors 398
show ipv6 route 399
show ipv6 route summary 401
traceroute ipv6 402

Chapter 15: Routing Commands 403
Introduction 403
ip route 404
ipv6 route 406
show ip route 408
show ip route database 410
show ip route summary 411
show ipv6 route 412
show ipv6 route summary 414

PART 4: Access and Security 415

Chapter 16: AAA Commands 416
Introduction 416
aaa accounting commands 418
aaa accounting login 420
aaa authentication download-portal 423
aaa authentication enable default group tacacs+ 425
aaa authentication enable default local 427
aaa authentication login 428
aaa authorization commands 431
aaa authorization config-commands 433
aaa group server 434
aaa local authentication attempts lockout-time 436
aaa local authentication attempts max-fail 437
aaa local authentication attempts max-fail remote-login-only 438
aaa login fail-delay 439
accounting login 440
authorization commands 441
clear aaa local user lockout 443
debug aaa 444
login authentication 445
proxy-port 446
radius-secure-proxy aaa 447
server (radsecproxy-aaa) 448
server mutual-authentication 450
server name-check 451
server trustpoint 452
show aaa local user locked 454
show aaa server group 456
show debugging aaa 457
show radius server group 458
undebug aaa 460

Chapter 17: Lightweight Directory Access Protocol (LDAP) Commands 461
Introduction 461
authentication (ldap-server) 463
base-dn 465
bind authenticate root-dn 466
deadtime (ldap-server) 467
debug ldap client 468
group-attribute 470
group-dn 471
host (ldap-server) 472
ldap-server 474
login-attribute 476
port (ldap-server) 478
retransmit (ldap-server) 479
search-filter 480
secure cipher (ldap-server) 482
secure mode (ldap-server) 484
secure trustpoint (ldap-server) 486
server (ldap-group) 487
show ldap server group 488
timeout (ldap-server) 490

Chapter 18: RADIUS Commands 491
Introduction 491
auth-mac-promiscuous 492
deadtime (RADIUS server group) 493
debug radius 494
ip radius require-message-authenticator 495
ip radius source-interface 496
radius-server deadtime 497
radius-server host 498
radius-server key 501
radius-server retransmit 502
radius-server timeout 504
server (RADIUS server group) 506
show debugging radius 508
show radius 509
show radius local-server auth-mac-promiscuous 512
undebug radius 513

Chapter 19: Public Key Infrastructure and Crypto Commands 514
Introduction 514
crypto key generate rsa 516
crypto key zeroize 517
crypto pki authenticate 518
crypto pki enroll 519
crypto pki enroll user 520
crypto pki export pem 522
crypto pki export pkcs12 523
crypto pki import pem 525
crypto pki import pkcs12 527
crypto pki trustpoint 528

enrollment (ca-trustpoint) 529
fingerprint (ca-trustpoint) 530
no crypto pki certificate 532
rsakeypair (ca-trustpoint) 533
show crypto key mypubkey rsa 534
show crypto pki certificates 535
show crypto pki enrollment user 537
show crypto pki trustpoint 538
show hash 539
subject-name (ca-trustpoint) 540

Chapter 20: TACACS+ Commands 542
Introduction 542
aaa authorization commands 543
aaa authorization config-commands 545
authorization commands 546
ip tacacs source-interface 548
show tacacs+ 549
tacacs-server host 551
tacacs-server key 553
tacacs-server timeout 554

PART 5: Network Management 555

Chapter 21: AMF and AMF Plus Commands 556
Introduction 556
application-proxy ip-filter 562
application-proxy quarantine-vlan 563
application-proxy redirect-url 564
application-proxy threat-protection 565
application-proxy threat-protection send-summary 567
application-proxy whitelist advertised-address 568
application-proxy whitelist enable 569
application-proxy whitelist protection tls 570
application-proxy whitelist server 571
application-proxy whitelist trustpoint (deprecated) 573
area-link 574
atmf-arealink 576
atmf-link 578
atmf amfplus-license-only 579
atmf area 581
atmf area password 583
atmf authorize 585
atmf authorize provision 587
atmf backup 589
atmf backup area-masters delete 590
atmf backup area-masters enable 591
atmf backup area-masters now 592
atmf backup area-masters synchronize 593
atmf backup bandwidth 594
atmf backup delete 595
atmf backup enable 596

atmf backup guests delete 597
atmf backup guests enable 598
atmf backup guests now 599
atmf backup guests synchronize 600
atmf backup now 601
atmf backup redundancy enable 603
atmf backup server 604
atmf backup stop 605
atmf backup synchronize 606
atmf cleanup 607
atmf container 608
atmf container login 609
atmf controller 610
atmf distribute firmware 611
atmf domain vlan 613
atmf enable 616
atmf group (membership) 617
atmf guest-class 619
atmf log-verbose 621
atmf management subnet 622
atmf management vlan 625
atmf master 627
atmf mtu 628
atmf network-name 629
atmf provision (interface) 630
atmf provision node 631
atmf reboot-rolling 633
atmf recover 637
atmf recover guest 639
atmf recover led-off 640
atmf recover over-eth 641
atmf recovery-server 642
atmf remote-login 644
atmf restricted-login 646
atmf retry guest-link 648
atmf secure-mode 649
atmf secure-mode certificate expire 651
atmf secure-mode certificate expiry 652
atmf secure-mode certificate renew 653
atmf secure-mode enable-all 654
atmf select-area 656
atmf topology-gui enable 657
atmf trustpoint 658
atmf virtual-crosslink 660
atmf virtual-link 662
atmf virtual-link description 665
atmf virtual-link protection 666
atmf working-set 668
bridge-group (amf-container) 670
clear application-proxy threat-protection 672
clear atmf links 673
clear atmf links virtual 674
clear atmf links statistics 675

clear atmf recovery-file 676
clear atmf secure-mode certificates 677
clear atmf secure-mode statistics 678
clone (amf-provision) 679
configure boot config (amf-provision) 681
configure boot system (amf-provision) 683
copy (amf-provision) 685
create (amf-provision) 686
debug atmf 688
debug atmf packet 690
delete (amf-provision) 692
discovery 694
description (amf-container) 696
erase factory-default 697
firmware-url 698
http-enable 700
identity (amf-provision) 702
license-cert (amf-provision) 704
locate (amf-provision) 706
log event-host 708
login-fallback enable 709
modeltype 710
service atmf-application-proxy 711
show application-proxy threat-protection 712
show application-proxy whitelist advertised-address 714
show application-proxy whitelist interface 715
show application-proxy whitelist server 717
show application-proxy whitelist supplicant 718
show atmf 720
show atmf area 724
show atmf area guests 727
show atmf area guests-detail 729
show atmf area nodes 731
show atmf area nodes-detail 733
show atmf area summary 735
show atmf authorization 736
show atmf backup 739
show atmf backup area 743
show atmf backup guest 745
show atmf container 747
show atmf detail 750
show atmf group 752
show atmf group members 754
show atmf guests 756
show atmf guests detail 758
show atmf links 761
show atmf links detail 763
show atmf links guest 772
show atmf links guest detail 774
show atmf links statistics 778
show atmf nodes 781
show atmf provision nodes 783
show atmf recovery-file 785

show atmf secure-mode . . . 786
show atmf secure-mode audit . . . 788
show atmf secure-mode audit link . . . 789
show atmf secure-mode certificates . . . 790
show atmf secure-mode sa . . . 793
show atmf secure-mode statistics . . . 796
show atmf tech . . . 798
show atmf virtual-links . . . 801
show atmf working-set . . . 803
show debugging atmf . . . 804
show debugging atmf packet . . . 805
show running-config atmf . . . 806
state . . . 807
switchport atmf-agentlink . . . 809
switchport atmf-arealink . . . 810
switchport atmf-crosslink . . . 812
switchport atmf-guestlink . . . 814
switchport atmf-link . . . 816
type atmf guest . . . 817
type atmf node . . . 818
undebug atmf . . . 820
username (atmf-guest) . . . 821

Chapter 22: STOAT Commands . . . 822
Introduction . . . 822
clear stoat collector session counters . . . 824
description (stoat-dest) . . . 825
key (stoat-dest) . . . 826
name-check (stoat-dest) . . . 827
service stoat . . . 828
show stoat collector . . . 829
show stoat destinations . . . 831
shutdown (stoat-dest) . . . 833
stoat collector enable . . . 834
stoat collector expiry-period . . . 835
stoat collector key . . . 836
stoat collector trustpoint . . . 838
stoat destination . . . 839
trustpoint (stoat-dest) . . . 841
unique-id . . . 842

Chapter 23: Dynamic Host Configuration Protocol (DHCP) Commands . . . 843
Introduction . . . 843
ip address dhcp . . . 844
ip dhcp-client default-route distance . . . 846
ip dhcp-client request vendor-identifying-specific . . . 848
ip dhcp-client vendor-identifying-class . . . 849
show counter dhcp-client . . . 850
show dhcp lease . . . 851

Chapter 24: DHCP for IPv6 (DHCPv6) Commands . . . 852
Introduction . . . 852

clear counter ipv6 dhcp-client 853
clear ipv6 dhcp client 854
ipv6 address dhcp 855
show counter ipv6 dhcp-client 857
show ipv6 dhcp interface 859

Chapter 25: Download Portal Commands 860
Introduction 860
aaa authentication download-portal 861
download-portal 863
download-portal reload 864
enable (download-portal) 865
file (download-portal) 866
http listen 868
http secure-listen 870
secure-listen (download-portal) 872
show download-portal 874
uri (download-portal) 875

Chapter 26: NTP Commands 876
Introduction 876
ntp authentication-key 877
ntp broadcastdelay 878
ntp master 879
ntp peer 880
ntp rate-limit 882
ntp restrict 883
ntp server 885
ntp source 887
show ntp associations 889
show ntp counters 891
show ntp counters associations 892
show ntp status 893

Chapter 27: SNMP Commands 894
Introduction 894
alias (interface) 896
debug snmp 897
show counter snmp-server 898
show debugging snmp 902
show running-config snmp 903
show snmp-server 904
show snmp-server community 905
show snmp-server group 906
show snmp-server trap 907
show snmp-server user 908
show snmp-server view 909
snmp trap link-status 910
snmp trap link-status suppress 911
snmp-server 913
snmp-server community 915
snmp-server contact 916

snmp-server enable trap 917
snmp-server engineID local 920
snmp-server engineID local reset 922
snmp-server group 923
snmp-server host 925
snmp-server legacy-ifadminstatus 927
snmp-server location 928
snmp-server source-interface 929
snmp-server startup-trap-delay 930
snmp-server user 931
snmp-server view 934
undebug snmp 935

Chapter 28: Mail (SMTP) Commands 936
Introduction 936
debug mail 937
delete mail 938
mail 939
mail from 941
mail smtpserver 942
mail smtpserver authentication 943
mail smtpserver port 945
mail smtpserver tls 947
show counter mail 948
show mail 949
undebug mail 950

Chapter 29: Secure Shell (SSH) Commands 951
Introduction 951
banner login (SSH) 953
clear ssh 954
crypto key destroy hostkey 955
crypto key destroy userkey 956
crypto key generate hostkey 957
crypto key generate userkey 959
crypto key pubkey-chain knownhosts 961
crypto key pubkey-chain userkey 963
debug ssh client 965
debug ssh server 966
service ssh 967
show banner login 969
show crypto key hostkey 970
show crypto key pubkey-chain knownhosts 972
show crypto key pubkey-chain userkey 974
show crypto key userkey 975
show running-config ssh 976
show ssh 978
show ssh client 980
show ssh server 981
show ssh server allow-users 983
show ssh server deny-users 984
ssh 985

ssh client 987
ssh client allow-legacy-ssh-rsa 989
ssh server 990
ssh server allow-legacy-ssh-rsa 992
ssh server allow-users 993
ssh server authentication 995
ssh server deny-users 997
ssh server max-auth-tries 999
ssh server resolve-host 1000
ssh server scp 1001
ssh server secure-algs 1002
ssh server secure-ciphers 1003
ssh server secure-hostkey 1004
ssh server secure-kex 1005
ssh server secure-mac 1006
ssh server sftp 1007
ssh server tcpforwarding 1008
undebug ssh client 1009
undebug ssh server 1010

Chapter 30: Trigger Commands 1011
Introduction 1011
active (trigger) 1013
day 1014
debug trigger 1016
description (trigger) 1017
repeat 1018
script 1019
show debugging trigger 1021
show running-config trigger 1022
show trigger 1023
test 1028
time (trigger) 1029
trap 1031
trigger 1032
trigger activate 1033
type atmf guest 1034
type atmf node 1035
type cpu 1037
type interface 1038
type linkmon-probe 1039
type log 1041
type memory 1042
type periodic 1043
type ping-poll 1044
type reboot 1045
type time 1046
undebug trigger 1047

Chapter 31: Ping-Polling Commands 1048
Introduction 1048
active (ping-polling) 1050

clear ping-poll 1051
critical-interval 1052
debug ping-poll 1053
description (ping-polling) 1054
fail-count 1055
ip (ping-polling) 1056
length (ping-poll data) 1057
normal-interval 1058
ping-poll 1059
sample-size 1060
show counter ping-poll 1062
show ping-poll 1064
source-ip 1068
timeout (ping polling) 1070
up-count 1071
undebug ping-poll 1072

PART 6: Virtual Private Networks (VPNs) 1073

Chapter 32: IPsec Commands 1074
Introduction 1074
clear isakmp sa 1076
crypto ipsec profile 1077
crypto isakmp key 1079
crypto isakmp peer 1082
crypto isakmp profile 1084
debug isakmp 1086
dpd-interval 1088
dpd-timeout 1089
interface tunnel (IPsec) 1090
lifetime (IPsec Profile) 1091
lifetime (ISAKMP Profile) 1092
no debug isakmp 1093
pfs 1094
rekey 1096
show debugging isakmp 1097
show interface tunnel (IPsec) 1098
show ipsec counters 1100
show ipsec peer 1101
show ipsec policy 1102
show ipsec profile 1103
show ipsec sa 1105
show isakmp counters 1106
show isakmp key (IPsec) 1107
show isakmp peer 1108
show isakmp profile 1109
show isakmp sa 1111
show tunnel inline-processing counters 1112
transform (IPsec Profile) 1114
transform (ISAKMP Profile) 1116
tunnel destination (IPsec) 1118
tunnel inline-processing 1120

tunnel local name (IPsec) 1121
tunnel local selector 1122
tunnel mode ipsec 1124
tunnel oper-status-control 1125
tunnel protection ipsec (IPsec) 1128
tunnel remote name (IPsec) 1129
tunnel remote selector 1130
tunnel security-reprocessing 1132
tunnel selector paired 1133
tunnel source (IPsec) 1134
undebug isakmp 1136
version (ISAKMP) 1137

Chapter 33: L2TPv3 Ethernet Pseudowire Commands 1138
Introduction 1138
interface tunnel (L2TPv3) 1139
l2tp unmanaged port 1140
show interface tunnel (L2TPv3) 1141
tunnel destination (L2TPv3) 1142
tunnel df 1144
tunnel local id 1145
tunnel mode l2tp v3 1146
tunnel protection ipsec 1147
tunnel remote id 1148
tunnel security-reprocessing 1149
tunnel source (L2TPv3) 1150

List of Commands

aaa accounting commands. 418
aaa accounting login. 420
aaa authentication download-portal 423
aaa authentication download-portal 861
aaa authentication enable default group tacacs+ 425
aaa authentication enable default local. 111
aaa authentication enable default local. 427
aaa authentication login 428
aaa authorization commands 431
aaa authorization commands 543
aaa authorization config-commands 433
aaa authorization config-commands 545
aaa group server. 434
aaa local authentication attempts lockout-time. 112
aaa local authentication attempts lockout-time. 436
aaa local authentication attempts max-fail remote-login-only 438
aaa local authentication attempts max-fail. 113
aaa local authentication attempts max-fail. 437
aaa login fail-delay. 114
aaa login fail-delay. 439
accounting login. 440
activate. 285
active (ping-polling) 1050
active (trigger). 1013
ageing-time 306

alias (interface) 896
application-proxy ip-filter 562
application-proxy quarantine-vlan 563
application-proxy redirect-url 564
application-proxy threat-protection send-summary 567
application-proxy threat-protection 565
application-proxy whitelist advertised-address 568
application-proxy whitelist enable 569
application-proxy whitelist protection tls 570
application-proxy whitelist server 571
application-proxy whitelist trustpoint (deprecated) 573
area-link 574
arp log 322
arp opportunistic-nd 325
arp 321
arp-loose-check 326
atmf amfplus-license-only 579
atmf area password 583
atmf area 581
atmf authorize provision 587
atmf authorize 585
atmf backup area-masters delete 590
atmf backup area-masters enable 591
atmf backup area-masters now 592
atmf backup area-masters synchronize 593
atmf backup bandwidth 594
atmf backup delete 595
atmf backup enable 596
atmf backup guests delete 597
atmf backup guests enable 598
atmf backup guests now 599
atmf backup guests synchronize 600
atmf backup now 601
atmf backup redundancy enable 603
atmf backup server 604

atmf backup stop 605
atmf backup synchronize 606
atmf backup 589
atmf cleanup 607
atmf container login 609
atmf container 608
atmf controller 610
atmf distribute firmware 611
atmf domain vlan 613
atmf enable 616
atmf group (membership) 617
atmf guest-class 619
atmf log-verbose 621
atmf management subnet 622
atmf management vlan 625
atmf master 627
atmf mtu 628
atmf network-name 629
atmf provision (interface) 630
atmf provision node 631
atmf reboot-rolling 633
atmf recover guest 639
atmf recover led-off 640
atmf recover over-eth 641
atmf recover 637
atmf recovery-server 642
atmf remote-login 644
atmf restricted-login 646
atmf retry guest-link 648
atmf secure-mode certificate expire 651
atmf secure-mode certificate expiry 652
atmf secure-mode certificate renew 653
atmf secure-mode enable-all 654
atmf secure-mode 649
atmf select-area 656

atmf topology-gui enable 55
atmf topology-gui enable 657
atmf trustpoint 658
atmf virtual-crosslink 660
atmf virtual-link description 665
atmf virtual-link protection 666
atmf virtual-link 662
atmf working-set 668
atmf-arealink 576
atmf-link 578
authentication (ldap-server) 463
auth-mac-promiscuous 492
authorization commands 441
authorization commands 546
banner display external-manager 156
banner exec 157
banner external-manager 159
banner login (SSH) 953
banner login (system) 161
banner motd 163
base-dn 465
bind authenticate root-dn 466
boot config-file backup 68
boot config-file 67
bridge 307
bridge-group (amf-container) 670
bridge-group 308
cd 69
clear aaa local user lockout 115
clear aaa local user lockout 443
clear application-proxy threat-protection 672
clear arp-cache 327
clear atmf links statistics 675
clear atmf links virtual 674
clear atmf links 673

clear atmf recovery-file 676
clear atmf secure-mode certificates 677
clear atmf secure-mode statistics....678
clear counter ipv6 dhcp-client....853
clear exception log 208
clear ipv6 dhcp client 854
clear ipv6 neighbors 363
clear isakmp sa 1076
clear line vty....116
clear log buffered....210
clear log permanent 211
clear log....209
clear ping-poll....1051
clear ssh....954
clear stoat collector session counters....824
clock set....165
clock summer-time date 166
clock summer-time recurring 168
clock timezone 170
clone (amf-provision) 679
configure boot config (amf-provision)....681
configure boot system (amf-provision) 683
configure terminal....44
copy (amf-provision)....685
copy (filename)....70
copy buffered-log 212
copy debug 72
copy permanent-log....213
copy running-config....73
copy startup-config....74
copy zmodem 75
create (amf-provision) 686
critical-interval 1052
crypto ipsec profile 1077
crypto isakmp key 1079

crypto isakmp peer 1082
crypto isakmp profile 1084
crypto key destroy hostkey....955
crypto key destroy userkey....956
crypto key generate hostkey 957
crypto key generate rsa 516
crypto key generate userkey 959
crypto key pubkey-chain knownhosts 961
crypto key pubkey-chain userkey....963
crypto key zeroize 517
crypto pki authenticate 518
crypto pki enroll user 520
crypto pki enroll 519
crypto pki export pem 522
crypto pki export pkcs12....523
crypto pki import pem 525
crypto pki import pkcs12....527
crypto pki trustpoint....528
day....1014
deadtime (ldap-server)....467
deadtime (RADIUS server group) 493
debug aaa....444
debug atmf packet 690
debug atmf....688
debug ip packet interface....328
debug isakmp 1086
debug ldap client....468
debug mail 937
debug ping-poll 1053
debug radius 494
debug snmp....897
debug ssh client 965
debug ssh server 966
debug trigger 1016
default log buffered 214

default log console 215
default log email 216
default log host 217
default log monitor 218
default log permanent 219
delete (amf-provision) 692
delete debug 77
delete mail 938
delete 76
description (amf-container) 696
description (interface) 289
description (ping-polling) 1054
description (stoat-dest) 825
description (trigger) 1017
dir 78
disable (Privileged Exec mode) 45
discovery 694
do 46
download-portal reload 864
download-portal 863
dpd-interval 1088
dpd-timeout 1089
echo 286
edit 80
enable (download-portal) 865
enable (Privileged Exec mode) 47
enable password 117
enable secret (deprecated) 119
encapsulation dot1q 316
end 49
enrollment (ca-trustpoint) 529
erase factory-default 697
erase factory-default 81
erase startup-config 82
exec-timeout 120

exit 50
fail-count 1055
file (download-portal) 866
fingerprint (ca-trustpoint) 530
firmware-url 698
group-attribute 470
group-dn 471
help 51
host (ldap-server) 472
hostname 171
http listen 868
http log webapi-requests 56
http port 57
http secure-listen 870
http secure-port 58
http trustpoint 59
http-enable 700
identity (amf-provision) 702
interface (to configure) 290
interface tunnel (IPsec) 1090
interface tunnel (L2TPv3) 1139
ip (ping-polling) 1056
ip address (IP Addressing and Protocol) 330
ip address dhcp 844
ip dhcp-client default-route distance 846
ip dhcp-client request vendor-identifying-specific 848
ip dhcp-client vendor-identifying-class 849
ip dns forwarding domain-list 351
ip domain-list 352
ip domain-lookup 353
ip domain-name 354
ip forwarding 332
ip icmp error-interval 333
ip icmp-timestamp 334
ip name-server 355

ip radius require-message-authenticator 495
ip radius source-interface 496
ip route 404
ip tacacs source-interface 548
ip tcp synack-retries 335
ip tcp-timestamp 336
ip tftp source-interface. 83
ip unreachables 337
ipv6 address autoconfig 365
ipv6 address dhcp 855
ipv6 address suffix 367
ipv6 address. 364
ipv6 enable. 368
ipv6 eui64-linklocal 370
ipv6 forwarding 371
ipv6 icmp error-interval 372
ipv6 nd accept-ra-default-routes 373
ipv6 nd accept-ra-pinfo 374
ipv6 nd current-hoplimit 375
ipv6 nd dns search-list 376
ipv6 nd dns-server 377
ipv6 nd managed-config-flag 378
ipv6 nd minimum-ra-interval. 379
ipv6 nd other-config-flag 380
ipv6 nd prefix. 381
ipv6 nd ra-interval 383
ipv6 nd ra-lifetime 384
ipv6 nd reachable-time 385
ipv6 nd retransmission-time 386
ipv6 nd route-information 387
ipv6 nd router-preference. 388
ipv6 nd suppress-ra 389
ipv6 opportunistic-nd. 390
ipv6 route 391
ipv6 route 406

ipv6 tftp source-interface 84
ipv6 unreachables 393
key (stoat-dest) 826
l2tp unmanaged port 1140
l3-filtering enable 310
ldap-server 474
length (asyn) 121
length (ping-poll data) 1057
license update file 151
license update online 152
license-cert (amf-provision) 704
lifetime (IPsec Profile) 1091
lifetime (ISAKMP Profile) 1092
line 122
locate (amf-provision) 706
log buffered (filter) 221
log buffered exclude 224
log buffered size 227
log buffered 220
log console (filter) 229
log console exclude 232
log console 228
log email (filter) 236
log email exclude 239
log email time 242
log email 235
log event-host 61
log event-host 708
log facility 244
log host (filter) 248
log host exclude 251
log host source 254
log host startup-delay 255
log host time 257
log host 246

log monitor (filter) 259
log monitor exclude 262
log permanent (filter) 266
log permanent exclude 269
log permanent size 272
log permanent 265
log trustpoint 274
login authentication 445
login-attribute 476
login-fallback enable 709
logout 52
log-rate-limit nsm 273
low-memory restart 172
mac-learning 311
mail from 941
mail smtpserver authentication 943
mail smtpserver port 945
mail smtpserver tls 947
mail smtpserver 942
mail 939
mkdir 85
modeltype 710
move debug 87
move 86
mtu 292
name-check (stoat-dest) 827
no crypto pki certificate 532
no debug all 173
no debug isakmp 1093
normal-interval 1058
ntp authentication-key 877
ntp broadcastdelay 878
ntp master 879
ntp peer 880
ntp rate-limit 882

ntp restrict 883
ntp server 885
ntp source....887
pfs 1094
ping ipv6....394
ping....339
ping-poll 1059
port (ldap-server)....478
privilege level 123
proxy-port....446
pwd....88
radius-secure-proxy aaa....447
radius-server deadtime 497
radius-server host 498
radius-server key 501
radius-server retransmit....502
radius-server timeout....504
reboot 175
rekey....1096
reload....176
repeat....1018
retransmit (ldap-server)....479
rmdir....89
rsakeypair (ca-trustpoint) 533
sample-size....1060
script....1019
search-filter 480
secure cipher (ldap-server)....482
secure mode (ldap-server) 484
secure trustpoint (ldap-server) 486
secure-listen (download-portal)....872
security-password forced-change 125
security-password history....124
security-password lifetime 126
security-password minimum-categories....128

security-password minimum-length....129
security-password min-lifetime-enforce....127
security-password reject-expired-pwd....130
security-password warning....131
server (ldap-group)....487
server (RADIUS server group)....506
server (radsecproxy-aaa)....448
server mutual-authentication....450
server name-check....451
server trustpoint....452
service advanced-vty....132
service atmf-application-proxy....711
service http....62
service password-encryption....133
service ssh....967
service statistics interfaces counter....294
service stoat....828
service telnet....134
show aaa local user locked....135
show aaa local user locked....454
show aaa server group....456
show application-proxy threat-protection....712
show application-proxy whitelist advertised-address....714
show application-proxy whitelist interface....715
show application-proxy whitelist server....717
show application-proxy whitelist supplicant....718
show arp....340
show atmf area guests....727
show atmf area guests-detail....729
show atmf area nodes....731
show atmf area nodes-detail....733
show atmf area summary....735
show atmf area....724
show atmf authorization....736
show atmf backup area....743

show atmf backup guest....745
show atmf backup....739
show atmf container....747
show atmf detail....750
show atmf group members....754
show atmf group....752
show atmf guests detail....758
show atmf guests....756
show atmf links detail....763
show atmf links guest detail....774
show atmf links guest....772
show atmf links statistics....778
show atmf links....761
show atmf nodes....781
show atmf provision nodes....783
show atmf recovery-file....785
show atmf secure-mode audit link....789
show atmf secure-mode audit....788
show atmf secure-mode certificates....790
show atmf secure-mode sa....793
show atmf secure-mode statistics....796
show atmf secure-mode....786
show atmf tech....798
show atmf virtual-links....801
show atmf working-set....803
show atmf....720
show banner external-manager....177
show banner login....969
show boot....90
show bridge macaddr....314
show bridge....312
show clock....178
show counter dhcp-client....850
show counter ipv6 dhcp-client....857
show counter log....275

show counter mail 948
show counter ping-poll 1062
show counter snmp-server 898
show cpu history 183
show cpu 180
show crypto key hostkey 970
show crypto key mypubkey rsa 534
show crypto key pubkey-chain knownhosts 972
show crypto key pubkey-chain userkey 974
show crypto key userkey 975
show crypto pki certificates 535
show crypto pki enrollment user 537
show crypto pki trustpoint 538
show debugging aaa 457
show debugging atmf packet 805
show debugging atmf 804
show debugging isakmp 1097
show debugging radius 508
show debugging snmp 902
show debugging trigger 1021
show debugging 185
show dhcp lease 851
show download-portal 874
show exception log 276
show file systems 93
show file 92
show hash 539
show hash 91
show history 53
show hosts 357
show http 63
show interface brief 298
show interface memory 186
show interface memory 299
show interface status 301

show interface tunnel (IPsec) 1098
show interface tunnel (L2TPv3) 1141
show interface 295
show ip domain-list 358
show ip domain-name 359
show ip flooding-nexthops 341
show ip forwarding 342
show ip interface 343
show ip name-server 360
show ip route database 410
show ip route summary 411
show ip route 408
show ip sockets 344
show ipsec counters 1100
show ipsec peer 1101
show ipsec policy 1102
show ipsec profile 1103
show ipsec sa 1105
show ipv6 dhcp interface 859
show ipv6 forwarding 396
show ipv6 interface 397
show ipv6 neighbors 398
show ipv6 route summary 401
show ipv6 route summary 414
show ipv6 route 399
show ipv6 route 412
show isakmp counters 1106
show isakmp key (IPsec) 1107
show isakmp peer 1108
show isakmp profile 1109
show isakmp sa 1111
show ldap server group 488
show license external 153
show log config 279
show log permanent 281

show log 277
show mail 949
show memory allocations 190
show memory history 192
show memory pools 193
show memory shared 194
show memory 188
show ntp associations 889
show ntp counters associations 892
show ntp counters 891
show ntp status 893
show ping-poll 1064
show privilege 137
show process 195
show radius local-server auth-mac-promiscuous 512
show radius server group 458
show radius 509
show reboot history 197
show router-id 198
show running-config atmf 806
show running-config interface 98
show running-config log 283
show running-config snmp 903
show running-config ssh 976
show running-config trigger 1022
show running-config unencrypted 100
show running-config 95
show security-password configuration 138
show security-password user 139
show snmp-server community 905
show snmp-server group 906
show snmp-server trap 907
show snmp-server user 908
show snmp-server view 909
show snmp-server 904

show ssh client 980
show ssh server allow-users 983
show ssh server deny-users 984
show ssh server 981
show ssh 978
show startup-config 101
show stoat collector 829
show stoat destinations 831
show system mac 200
show system serialnumber 201
show system 199
show tacacs+ 549
show tech-support 202
show telnet 140
show trigger 1023
show tunnel inline-processing counters 1112
show users 141
show version 102
shutdown (stoat-dest) 833
shutdown 303
snmp trap link-status suppress 911
snmp trap link-status 910
snmp-server community 915
snmp-server contact 916
snmp-server enable trap 917
snmp-server engineID local reset 922
snmp-server engineID local 920
snmp-server group 923
snmp-server host 925
snmp-server legacy-ifadminstatus 927
snmp-server location 928
snmp-server source-interface 929
snmp-server startup-trap-delay 930
snmp-server user 931
snmp-server view 934

snmp-server 913
software-upgrade 103
source-ip 1068
ssh client allow-legacy-ssh-rsa 989
ssh client 987
ssh server allow-legacy-ssh-rsa 992
ssh server allow-users 993
ssh server authentication 995
ssh server deny-users 997
ssh server max-auth-tries 999
ssh server resolve-host 1000
ssh server scp 1001
ssh server secure-algs 1002
ssh server secure-ciphers 1003
ssh server secure-hostkey 1004
ssh server secure-kex 1005
ssh server secure-mac 1006
ssh server sftp 1007
ssh server tcpforwarding 1008
ssh server 990
ssh 985
state 807
stoat collector enable 834
stoat collector expiry-period 835
stoat collector key 836
stoat collector trustpoint 838
stoat destination 839
strict-user-process-control force 105
strict-user-process-control force 143
strict-user-process-control 104
strict-user-process-control 142
subject-name (ca-trustpoint) 540
switchport atmf-agentlink 809
switchport atmf-arealink 810
switchport atmf-crosslink 812

switchport atmf-guestlink. 814
switchport atmf-link 816
tacacs-server host 551
tacacs-server key 553
tacacs-server timeout 554
tcpdump 347
telnet server 145
telnet 144
terminal length 146
terminal monitor 204
terminal resize 147
test 1028
time (trigger) 1029
timeout (ldap-server) 490
timeout (ping polling) 1070
traceroute ipv6 402
traceroute 348
transform (IPsec Profile) 1114
transform (ISAKMP Profile) 1116
trap 1031
trigger activate 1033
trigger 1032
trustpoint (stoat-dest) 841
tunnel destination (IPsec) 1118
tunnel destination (L2TPv3) 1142
tunnel df 1144
tunnel inline-processing 1120
tunnel local id 1145
tunnel local name (IPsec) 1121
tunnel local selector 1122
tunnel mode ipsec 1124
tunnel mode l2tp v3 1146
tunnel oper-status-control 1125
tunnel protection ipsec (IPsec) 1128
tunnel protection ipsec 1147

tunnel remote id....1148
tunnel remote name (IPsec)....1129
tunnel remote selector....1130
tunnel security-reprocessing....1132
tunnel security-reprocessing....1149
tunnel selector paired....1133
tunnel source (IPsec)....1134
tunnel source (L2TPv3)....1150
type atmf guest....1034
type atmf guest....817
type atmf node....1035
type atmf node....818
type cpu....1037
type interface....1038
type linkmon-probe....1039
type log....1041
type memory....1042
type periodic....1043
type ping-poll....1044
type reboot....1045
type time....1046
undebug aaa....460
undebug all....205
undebug atmf....820
undebug ip packet interface....349
undebug isakmp....1136
undebug mail....950
undebug ping-poll....1072
undebug radius....513
undebug snmp....935
undebug ssh client....1009
undebug ssh server....1010
undebug trigger....1047
unique-id....842
up-count....1071

uri (download-portal) 875
username (atmf-guest) 821
username 148
version (ISAKMP) 1137
wait 287
write file 106
write memory 107
write terminal 108

Part 1: Setup and Troubleshooting

1 CLI Navigation Commands

Introduction

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

Command List

- "configure terminal" on page 44
- "disable (Privileged Exec mode)" on page 45
- "do" on page 46
- "enable (Privileged Exec mode)" on page 47
- "end" on page 49
- "exit" on page 50
- "help" on page 51
- "logout" on page 52
- "show history" on page 53

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 (deprecated) commands. If no password is specified then only users with the maximum privilege level set with the username command can assess Privileged Exec mode.

Syntax

```
enable [<privilege-level>]
```

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

Mode User Exec

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

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

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

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

```
awplus> enable
awplus#
```

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

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

```
awplus> enable 7
awplus#
```

Related commands

disable (Privileged Exec mode)

enable password

enable secret (deprecated)

exit

service password-encryption

username

end

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

Syntax

```
end
```

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

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

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

Related commands

disable (Privileged Exec mode)

enable (Privileged Exec mode)

exit

exit

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

Syntax

```
exit
```

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

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

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

Related commands

disable (Privileged Exec mode)

enable (Privileged Exec mode)

end

help

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

Syntax

```
help
```

Mode All command modes

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

```
awplus# help
```

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

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

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

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

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

logout

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

Syntax

```
logout
```

Mode User Exec and Privileged Exec

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

```
awplus# logout
```

show history

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

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

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show history
```

Mode User Exec and Privileged Exec

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

```
awplus# show history
```

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

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

2 Vista Manager EX Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure your device so it can be monitored and managed by Vista Manager EX™.

Command List

- "atmf topology-gui enable" on page 55
- "http log webapi-requests" on page 56
- "http port" on page 57
- "http secure-port" on page 58
- "http trustpoint" on page 59
- "log event-host" on page 61
- "service http" on page 62
- "show http" on page 63

atmf topology-gui enable

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

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

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

Syntax

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

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

Mode Global Configuration mode

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

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

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

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

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

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

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

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

Related commands atmf enable

log event-host

service http

http log webapi-requests

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

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

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

Syntax

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

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

Default Web API request logging is disabled.

Mode Global Configuration

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

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

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

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

Related commands http port

service http

show log

Command changes Version 5.4.8-1.1: command added

http port

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

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

Syntax

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

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

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

Mode Global Configuration

Usage notes Do not configure the HTTP port to be the same as the HTTPS port.

Note that the device will redirect from HTTP to HTTPS unless you have disabled HTTPS access, which we do not recommend doing.

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

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

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

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

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

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

Related commands http secure-port

service http

show http

Command changes Version 5.4.7-2.4: command added on AR-Series devices

Version 5.4.8-0.2: command added on AlliedWare Plus switches

http secure-port

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

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

Syntax

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

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

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

Mode Global Configuration

Usage notes Do not configure the HTTPS port to be the same as the HTTP port.

Note that if you are using Vista Manager EX and need to change the HTTPS port, you must use certificate-based authorization in Vista Manager EX. See the Vista Manager EX Installation Guide for instructions.

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

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

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

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

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

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

Related commands

http port

service http

show http

Command changes

Version 5.4.7-1.1: command added on AR-Series devices

Version 5.4.7-2.4: **none** parameter added

Version 5.4.8-0.2: command added on AlliedWare Plus switches

http trustpoint

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

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

Syntax

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

Parameter	Description
<trustpoint-name>	Name of trustpoint

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

Mode Global Configuration

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

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

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

Create the root and server certificates for this trustpoint:

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

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

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

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

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

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

Related commands

crypto pki trustpoint

show crypto pki certificates

show crypto pki trustpoint

Command changes

Version 5.5.1-2.1: command added

log event-host

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

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

Syntax

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

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

Default Log events are disabled by default.

Mode Global Configuration

Usage notes Event hosts are set so syslog sends the messages out as they come.

Note that there is a difference between log event and log host messages:

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

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

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

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

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

Related commands atmf topology-gui enable

service http

Overview Use this command to enable the HTTP (Hypertext Transfer Protocol) service.

This service is required to support Vista Manager EX™.

Use the **no** variant of this command to disable the HTTP feature.

Syntax

```
service http
no service http
```

Default Enabled

Mode Global Configuration

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

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

To disable the HTTP service, use the following commands:

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

Related commands show http

show http

Overview This command shows the HTTP server settings.

Syntax

```
show http
```

Mode User Exec and Privileged Exec

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

```
awplus# show http
```

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

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

Web GUI Information
-------------------------------------------------------------
GUI file in use                : awplus-gui_551_23.gui

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

Related commands clear line vty

service http

3 File and Configuration Management Commands

Introduction

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

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

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

Valid characters

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

1) uppercase letters: A to Z

2) lowercase letters: a to z

3) digits: 0 to 9

4) special symbols: most printable ASCII characters not included in the previous three categories, including the following characters:

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

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

Syntax for directory listings

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

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

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

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

Command list

- "boot config-file" on page 67
- "boot config-file backup" on page 68
- "cd" on page 69
- "copy (filename)" on page 70
- "copy debug" on page 72
- "copy running-config" on page 73

- "copy startup-config" on page 74
- "copy zmodem" on page 75
- "delete" on page 76
- "delete debug" on page 77
- "dir" on page 78
- "edit" on page 80
- "erase factory-default" on page 81
- "erase startup-config" on page 82
- "ip tftp source-interface" on page 83
- "ipv6 tftp source-interface" on page 84
- "mkdir" on page 85
- "move" on page 86
- "move debug" on page 87
- "pwd" on page 88
- "rmdir" on page 89
- "show boot" on page 90
- "show hash" on page 91
- "show file" on page 92
- "show file systems" on page 93
- "show running-config" on page 95
- "show running-config interface" on page 98
- "show running-config unencrypted" on page 100
- "show startup-config" on page 101
- "show version" on page 102
- "software-upgrade" on page 103
- "strict-user-process-control" on page 104
- "strict-user-process-control force" on page 105
- "write file" on page 106
- "write memory" on page 107
- "write terminal" on page 108

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 notes For an explanation of the configuration fallback order, see the File Management Feature Overview and Configuration Guide.

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

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

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

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

Related commands boot config-file backup

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 notes For an explanation of the configuration fallback order, see the File Management Feature Overview and Configuration Guide.

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

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

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

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

Related commands boot config-file

show boot

cd

Overview This command changes the current working directory.

Syntax

```
cd <directory-name>
```

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

Mode Privileged Exec

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

```
awplus# cd images
```

Related commands

dir

pwd

show file systems

copy (filename)

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

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

Syntax

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

Parameter	Description
`force`	This parameter forces the copy command to overwrite the destination file, if it already exists, without prompting the user for confirmation.
<source-name>	The filename and path of the source file. See Introduction on page 64 for valid syntax.
<destination-name>	The filename and path for the destination file. See Introduction on page 64 for valid syntax.

Mode Privileged Exec

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

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

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

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

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

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

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

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

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

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

Related commands

copy zmodem

copy buffered-log

copy permanent-log

show file systems

copy debug

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

Syntax

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

Parameter	Description
<destination-name>	The filename and path where you would like the debug output saved. See Introduction on page 64 for valid syntax.
<source-name>	The filename and path where the debug output originates. See the Introduction to this chapter for valid syntax.

Mode Privileged Exec

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

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

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

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

Related commands

delete debug

move debug

copy running-config

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

Syntax

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

Parameter	Description
<source-name>	The filename and path of a configuration file. This must be a valid configuration file with a **.cfg** filename extension. Specify this when you want the script in the file to become the new running-config. See Introduction on page 64 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 64 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 64 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 64 for valid syntax.

Mode Privileged Exec

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

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

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

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

Related commands copy running-config

copy zmodem

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

Syntax

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

Parameter	Description
<source-name>	The filename and path of the source file. See Introduction on page 64 for valid syntax.

Mode Privileged Exec

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

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

Related commands copy (filename)

show file systems

delete

Overview This command deletes files or directories.

Syntax `delete [force] [recursive] <filename>`

Parameter	Description
`force`	Ignore nonexistent filenames and never prompt before deletion.
`recursive`	Remove the contents of directories recursively.
`<filename>`	The filename and path of the file to delete. See Introduction on page 64 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 64 for valid URL syntax.

Mode Privileged Exec

Example To delete debug output, use the following command:

```
awplus# delete debug
```

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

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

Related commands

copy debug

move debug

dir

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

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

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

Mode Privileged Exec

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

```
awplus# dir
```

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

```
awplus# dir flash
```

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

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

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

```
awplus# dir sort name
```

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

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

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

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

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

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

Related commands

cd

mkdir

pwd

edit

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

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

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

For information about using the editor, including control sequences, see the File Management Feature Overview and Configuration Guide.

Syntax

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

Parameter	Description
<filename>	The name of a file in the local Flash filesystem.
<remote-file>	The filename and path of the remote file. See Introduction on page 64 for valid syntax.

Mode Privileged Exec

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

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

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

```
awplus# edit
```

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

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

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

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

Related commands

copy (filename)

dir

mkdir

show file

erase factory-default

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

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

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

Syntax

```
erase factory-default
```

Mode Privileged Exec

Usage notes This command is an alias to the atmf cleanup command.

Example To erase data, use the command:

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

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

Related commands atmf cleanup

erase startup-config

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

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

Syntax

```
erase startup-config
```

Mode Privileged Exec

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

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

Related commands

boot config-file backup

copy running-config

copy startup-config

show boot

ip tftp source-interface

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

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

Syntax

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

Parameter	Description
<interface>	The VLAN that TFTP requests originate from. The device will use the IP address of this interface as its source IP address.
<ip-add>	The IP address that TFTP requests originate from, in dotted decimal format.

Default There is no default source specified.

Mode Global Configuration

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

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

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

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

Related commands copy (filename)

ipv6 tftp source-interface

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

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

Syntax

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

Parameter	Description
<interface>	The VLAN that TFTP requests originate from. The device will use the IPv6 address of this interface as its source IPv6 address.
<ipv6-add>	The IPv6 address that TFTP requests originate from, in the format x:x::x:x, for example, 2001:db8::8a2e:7334.

Default There is no default source specified.

Mode Global Configuration

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

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

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

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

Related commands copy (filename)

mkdir

Overview This command makes a new directory.

Syntax

```
mkdir <name>
```

Parameter	Description
<name>	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
<source-name>	The filename and path of the source file. See Introduction on page 64 for valid syntax.
<destination-name>	The filename and path of the destination file. See Introduction on page 64 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}
```

Parameter	Description
<destination-name>	The filename and path where you would like the debug output moved to. See Introduction on page 64 for valid syntax.

Mode Privileged Exec

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

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

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

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

Related commands

copy debug

delete debug

pwd

Overview This command prints the current working directory.

Syntax

```
pwd
```

Mode Privileged Exec

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

```
awplus# pwd
```

Related commands cd

rmdir

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

Syntax

```
rmdir [force] <name>
```

Parameter	Description
`force`	Optional keyword that allows you to delete directories that are not empty and 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 create a directory called "level1" containing a subdirectory called "level2", and then force the removal of both directories, use the commands:

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

Related commands

cd

dir

mkdir

pwd

show boot

Overview This command displays the current boot configuration.

Syntax

```
show boot
```

Mode Privileged Exec

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

```
awplus# show boot
```

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

```
awplus#show boot
Boot configuration
-----------------------------------------------------------------
Current software   : vaa-5.5.4-2.1.iso
Boot location      : Local
Default boot config: flash:/default.cfg
Current boot config: flash:/my.cfg (file exists)
Backup  boot config: flash:/backup.cfg (file not found)
```

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

Parameter	Description
`Current software`	The current software release that the device is using.
`Boot location`	The location where the current software release is stored; either local or CD/DVD.
`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.

Related commands boot config-file backup

show hash

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

Syntax

```
show hash <filename>
```

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

Mode Privileged Exec

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

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

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

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

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

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

Command changes Version 5.5.3-0.1: command added

show file

Overview This command displays the contents of a specified file.

Syntax

```
show file <filename>
```

Parameter	Description
<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

show file systems

show file systems

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

Syntax
```
show file systems
```

Mode Privileged Exec

Examples To display the file systems, use the command:

```
awplus# show file systems
```

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

```
awplus#show file systems

 Size(b)   Free(b)   Type    Flags  Prefixes   S/D/V    Lcl/Ntwk  Avail
-----------------------------------------------------------------------
   4.6G      4.0G   flash     rw   flash:     static   local      Y
      -         -   system    rw   system:    virtual  local      -
  10.0M      9.6M   debug     rw   debug:     static   local      Y
      -         -   fserver   rw   fserver:   dynamic  network    N
      -         -   tftp      rw   tftp:      -        network    -
      -         -   scp       rw   scp:       -        network    -
      -         -   sftp      ro   sftp:      -        network    -
      -         -   http      ro   http:      -        network    -
      -         -   rsync     rw   rsync:     -        network    -
```

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

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

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

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

Related commands

edit

show file

show running-config

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

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

- To display only lines that contain a particular word, enter:

```
| include <word>
```

- To start the display at the first line that contains a particular word, enter:

```
| begin <word>
```

- To save the output to a file, enter:

```
> <filename>
```

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

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

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

Parameter	Description	
	switch	Switch configuration
	web-control	Web Control configuration

Mode Privileged Exec and Global Configuration

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

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

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

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

...

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

Related commands

copy running-config

show running-config interface

show running-config unencrypted

show running-config interface

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

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

Syntax

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

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

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

Mode Privileged Exec and Global Configuration

Default Displays information for all protocols on all interfaces

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

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

Output Figure 3-9: Example output from a **show running-config interface eth0** command

```
awplus#show running-config interface eth0
!
interface eth0
 encapsulation dot1q 2
 encapsulation dot1q 3
!
```

Related commands copy running-config

show running-config

show running-config unencrypted

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

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

Syntax

```
show running-config unencrypted
```

Mode Privileged Exec

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

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

Related commands show running-config

Command changes Version 5.5.3-2.1: command added

show startup-config

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

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show startup-config
```

Mode Privileged Exec

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

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

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

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

...

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

Related commands
boot config-file backup
copy running-config
copy startup-config
erase startup-config
show boot

show version

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

Syntax

```
show version
```

Mode User Exec and Privileged Exec

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

```
awplus# show version
```

Related commands show boot

software-upgrade

Overview Use this command to update the firmware on your AMF Cloud installation.

Syntax

```
software-upgrade <filename>
```

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

Mode Privileged Exec

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

This command only works if your AMF Cloud ISO image is attached as a virtual hard drive on your virtual machine.

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

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

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

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

```
awplus# dir
```

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

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

```
awplus# software-upgrade vaa-5.5.4-2.1.iso
```

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

3) Reboot with the new firmware.

```
awplus# reboot
```

Related commands show boot

strict-user-process-control

Overview Use this command to enable Strict User Process Control.

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

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

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

Syntax

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

Default Disabled.

Mode Global Configuration

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

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

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

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

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

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

Related commands show running-config

strict-user-process-control force

Command changes Version 5.5.2-2.1: command added

strict-user-process-control force

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

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

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

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

Syntax

```
strict-user-process-control force
```

Default Disabled.

Mode Global Configuration

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

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

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

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

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

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

Related commands show running-config

strict-user-process-control

Command changes Version 5.5.4-1.8: command added

write file

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

Syntax

```
write [file]
```

Mode Privileged Exec

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

```
awplus# write file
```

Related commands

copy running-config

write memory

show running-config

write memory

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

Syntax

```
write [memory]
```

Mode Privileged Exec

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

```
awplus# write memory
```

Related commands

copy running-config

write file

show running-config

write terminal

Overview This command displays the current configuration of the device. This command is a synonym of the show running-config command.

Syntax

```
write terminal
```

Mode Privileged Exec

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

```
awplus# write terminal
```

Related commands show running-config

4 User Access Commands

Introduction

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

Command List

- "aaa authentication enable default local" on page 111
- "aaa local authentication attempts lockout-time" on page 112
- "aaa local authentication attempts max-fail" on page 113
- "aaa login fail-delay" on page 114
- "clear aaa local user lockout" on page 115
- "clear line vty" on page 116
- "enable password" on page 117
- "enable secret (deprecated)" on page 119
- "exec-timeout" on page 120
- "length (asyn)" on page 121
- "line" on page 122
- "privilege level" on page 123
- "security-password history" on page 124
- "security-password forced-change" on page 125
- "security-password lifetime" on page 126
- "security-password min-lifetime-enforce" on page 127
- "security-password minimum-categories" on page 128
- "security-password minimum-length" on page 129
- "security-password reject-expired-pwd" on page 130
- "security-password warning" on page 131

- "service advanced-vty" on page 132
- "service password-encryption" on page 133
- "service telnet" on page 134
- "show aaa local user locked" on page 135
- "show privilege" on page 137
- "show security-password configuration" on page 138
- "show security-password user" on page 139
- "show telnet" on page 140
- "show users" on page 141
- "strict-user-process-control" on page 142
- "strict-user-process-control force" on page 143
- "telnet" on page 144
- "telnet server" on page 145
- "terminal length" on page 146
- "terminal resize" on page 147
- "username" on page 148

aaa authentication enable default local

Overview This command enables local privilege level authentication.

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

Syntax

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

Default Local privilege level authentication is enabled by default.

Mode Global Configuration

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

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

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

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

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

Related commands

aaa authentication login

enable (Privileged Exec mode)

enable password

enable secret (deprecated)

aaa local authentication attempts lockout-time

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

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

Syntax

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

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

Mode Global Configuration

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

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

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

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

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

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

Related commands

aaa local authentication attempts max-fail

aaa local authentication attempts max-fail remote-login-only

clear aaa local user lockout

aaa local authentication attempts max-fail

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

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

Syntax

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

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

Mode Global Configuration

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

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

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

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

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

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

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

Related commands

aaa local authentication attempts lockout-time

aaa local authentication attempts max-fail remote-login-only

clear aaa local user lockout

aaa login fail-delay

Overview Use this command to configure the minimum time period between failed login attempts. This setting applies to login attempts via the console, SSH and Telnet.

Use the **no** variant of this command to reset the minimum time period to its default value.

Syntax

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

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

Default 1 second

Mode Global configuration

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

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

Related commands

aaa authentication login

aaa local authentication attempts lockout-time

clear aaa local user lockout

clear aaa local user lockout

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

Syntax

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

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

Mode Privileged Exec

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

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

To unlock all user accounts use the following command:

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

Related commands aaa local authentication attempts lockout-time

clear line vty

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

Syntax

```
clear line vty <0-32>
```

Parameter	Description
<0-32>	Line number

Mode Privileged Exec

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

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

Related commands

privilege level

line

show telnet

show users

enable password

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

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

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

Syntax

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

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

Default Level 15

Mode Global Configuration

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

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

The device stores passwords in hashed form in configuration files, unless you disable service password-encryption.

Related commands

enable (Privileged Exec mode)

enable secret (deprecated)

service password-encryption

privilege level

show privilege

username

show running-config

enable secret (deprecated)

Overview This command has been deprecated. It has been replaced by the enable password command.

exec-timeout

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

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

Syntax

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

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

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

Mode Line Configuration

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

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

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

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

Related commands

line

service telnet

show running-config

length (asyn)

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

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

Syntax

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

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

Mode Line Configuration

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

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

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

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

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

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

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

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

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

Related commands terminal resize

terminal length

line

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

Syntax

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

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

Mode Global Configuration

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

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

- issuing a clear line console command
- issuing a reboot command
- logging out of the current session

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

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

Related commands

accounting login

clear line vty

length (asyn)

login authentication

privilege level

privilege level

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

Syntax

```
privilege level <1-15>
```

Mode Line Configuration

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

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

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

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

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

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

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

Related commands

enable password

line

show privilege

username

security-password history

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

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

Syntax

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

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

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

Mode Global Configuration

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

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

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

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

Related commands

security-password forced-change

security-password lifetime

security-password min-lifetime-enforce

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

security-password warning

show running-config security-password

show security-password configuration

show security-password user

security-password forced-change

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

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

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

Syntax

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

Default The forced-change feature is disabled by default.

Mode Global Configuration

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

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

Related commands

security-password history

security-password lifetime

security-password min-lifetime-enforce

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

security-password warning

show running-config security-password

show security-password configuration

show security-password user

security-password lifetime

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

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

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

Syntax

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

Parameter	Description
<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
```

Related commands

security-password forced-change

security-password history

security-password min-lifetime-enforce

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

security-password warning

show running-config security-password

show security-password configuration

show security-password user

security-password min-lifetime-enforce

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

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

Syntax

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

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

Default By default, no minimum lifetime is enforced.

Mode Global Configuration

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

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

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

Related commands

security-password forced-change

security-password history

security-password lifetime

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

security-password warning

show running-config security-password

show security-password configuration

show security-password user

Command changes Version 5.4.7-0.2: command added

security-password minimum-categories

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

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

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

Syntax

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

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

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

Mode Global Configuration

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

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

Related commands

security-password forced-change

security-password history

security-password lifetime

security-password min-lifetime-enforce

security-password minimum-length

security-password reject-expired-pwd

security-password warning

show running-config security-password

show security-password configuration

show security-password user

security-password minimum-length

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

Syntax

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

Parameter	Description
<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
```

Related commands

security-password forced-change

security-password history

security-password lifetime

security-password min-lifetime-enforce

security-password minimum-categories

security-password reject-expired-pwd

security-password warning

show running-config security-password

show security-password configuration

show security-password user

security-password reject-expired-pwd

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

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

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

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

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

Syntax

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

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

Mode Global Configuration

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

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

Related commands

security-password forced-change

security-password history

security-password lifetime

security-password min-lifetime-enforce

security-password minimum-categories

security-password minimum-length

security-password warning

show running-config security-password

show security-password configuration

show security-password user

security-password warning

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

Note that the warning period cannot be set unless the lifetime feature is enabled with the security-password lifetime command.

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

Syntax

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

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

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

Mode Global Configuration

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

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

Related commands

security-password forced-change

security-password history

security-password lifetime

security-password min-lifetime-enforce

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

show running-config security-password

show security-password configuration

show security-password user

service advanced-vty

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

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

Syntax

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

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

Mode Global Configuration

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

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

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

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

service password-encryption

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

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

Syntax

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

Mode Global Configuration

Example

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

Validation Commands show running-config

Related commands enable password

service telnet

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

The server listens on port 23, unless you have changed the port by using the privilege level command.

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

Syntax

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

Default The IPv4 and IPv6 telnet servers are enabled by default.

The configured telnet port is TCP port 23 by default.

Mode Global Configuration

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

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

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

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

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

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

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

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

Related commands clear line vty

show telnet

telnet server

show aaa local user locked

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

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

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

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

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

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

In the Valid column:

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

Syntax
```
show aaa local user locked
```

Mode User Exec and Privileged Exec

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

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

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

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

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

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

Related commands

aaa local authentication attempts lockout-time

aaa local authentication attempts max-fail

clear aaa local user lockout

show privilege

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

Syntax

```
show privilege
```

Mode User Exec and Privileged Exec

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

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

```
awplus# show privilege
```

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

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

Related commands privilege level

show security-password configuration

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

Syntax

```
show security-password configuration
```

Mode Privileged Exec

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

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

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

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

Related commands

security-password forced-change

security-password history

security-password lifetime

security-password min-lifetime-enforce

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

security-password warning

show security-password user

show security-password user

Overview This command displays user account and password information for all users.

Syntax

```
show security-password user
```

Mode Privileged Exec

Example To display the system users' remaining lifetime or last password change, use the command:

```
awplus# show security-password user
```

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

```
User account and password information

UserName          Privilege Last-PWD-Change   Remaining-lifetime
------------------------------------------------------------------
manager           15          4625 day(s) ago   No Expiry
bob15             15             0 day(s) ago   30 days
ted7              7              0 day(s) ago   No Expiry
mike1             1              0 day(s) ago   No Expiry
```

Related commands

security-password forced-change

security-password history

security-password lifetime

security-password min-lifetime-enforce

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

security-password warning

show security-password configuration

show telnet

Overview This command shows the Telnet server settings.

Syntax

```
show telnet
```

Mode User Exec and Privileged Exec

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

```
awplus# show telnet
```

Output Figure 4-5: Example output from the **show telnet** command

```
Telnet Server Configuration
-------------------------------------------------------------
Telnet server               : Enabled
Protocol                    : IPv4,IPv6
Port                        : 23
```

Related commands

clear line vty

service telnet

show users

telnet server

show users

Overview This command shows information about the users who are currently logged into the device.

Syntax

```
show users
```

Mode User Exec and Privileged Exec

Example To show the users currently connected to the device, use the command:

```
awplus# show users
```

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

```
Line     User             Host(s)  Idle      Location        Priv Idletime Timeout
con 0    manager          idle     00:00:00  ttyS0           15   10       N/A
vty 0    bob              idle     00:00:03  172.16.11.3     1    0        5
```

Table 1: Parameters in the output of the **show users** command

Parameter	Description
Line	Console port user is connected to.
User	Login name of user.
Host(s)	Status of the host the user is connected to.
Idle	How long the host has been idle.
Location	URL location of user.
Priv	The privilege level in the range 1 to 15, with 15 being the highest.
Idletime	The time interval the device waits for user input from either a console or VTY connection.
Timeout	The time interval before a server is considered unreachable.

strict-user-process-control

Overview Use this command to enable Strict User Process Control.

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

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

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

Syntax

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

Default Disabled.

Mode Global Configuration

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

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

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

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

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

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

Related commands show running-config

strict-user-process-control force

Command changes Version 5.5.2-2.1: command added

strict-user-process-control force

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

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

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

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

Syntax

```
strict-user-process-control force
```

Default Disabled.

Mode Global Configuration

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

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

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

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

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

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

Related commands show running-config

strict-user-process-control

Command changes Version 5.5.4-1.8: command added

telnet

Overview Use this command to open a telnet session to a remote device.

Syntax

```
telnet {<hostname>|[ip] <ipv4-addr>|[ipv6] <ipv6-addr>}
[<port>]
```

Parameter	Description
<hostname>	The host name of the remote system.
ip	Keyword used to specify the IPv4 address or host name of a remote system.
<ipv4-addr>	An IPv4 address of the remote system.
ipv6	Keyword used to specify the IPv6 address of a remote system
<ipv6-addr>	Placeholder for an IPv6 address in the format x:x::x:x, for example, 2001:db8::8a2e:7334
<port>	Specify a TCP port number (well known ports are in the range 1-1023, registered ports are 1024-49151, and private ports are 49152-65535).

Mode User Exec and Privileged Exec

Examples To connect to TCP port 2602 on the device at 10.2.2.2, use the command:

```
awplus# telnet 10.2.2.2 2602
```

To connect to the telnet server host.example, use the command:

```
awplus# telnet host.example
```

To connect to the telnet server host.example on TCP port 100, use the command:

```
awplus# telnet host.example 100
```

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 notes When the user's terminal size is changed, then a remote session via SSH or TELNET adjusts the terminal size automatically. However, this cannot normally be done automatically for a serial or console port. This command automatically adjusts the terminal size for a serial or console port.

Examples The following example automatically adjusts the number of rows shown on the console:

```
awplus# terminal resize
```

Related commands length (asyn)

terminal length

username

Overview This command creates or modifies a user to assign a privilege level and a password.

NOTE: *The default username privilege level of 1 is not shown in running-config output. Any username privilege level that has been modified from the default is shown.*

Syntax

```
username <name> privilege <1-15> [password [8] <password>]
username <name> password [8] <password>
no username <name>
```

Parameter	Description	
`<name>`	The login name for the user. Do not use punctuation marks such as single quotes (‘ ’), double quotes (“ ”), or colons (:) with the user login name.	
`privilege`	The user’s privilege level. Use the privilege levels to set the access rights for each user.	
	<1-15>	A privilege level: either 1-14 (limited access) or 15 (full access). A user with privilege level 1-14 can only access higher privilege levels if an enable password has been configured for the level the user tries to access and the user enters that password. A user at privilege level 1 can access the majority of show commands. A user at privilege level 7 can access the majority of show commands including platform show commands. Privilege Level 15 (to access the Privileged Exec command mode) is required to access configuration commands as well as show commands in Privileged Exec.
`password`	A password that the user must enter when logging in.	
	`8`	The parameter **8** means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form. Note that the user needs to enter the plain-text version of the password when logging in.
	<password>	The user’s password. The password can be up to 32 characters in length and include characters from up to four categories. The password categories are: • uppercase letters: A to Z • lowercase letters: a to z • digits: 0 to 9 • special symbols: all printable ASCII characters not included in the previous three categories. The question mark ? cannot be used as it is reserved for help functionality.

Mode Global Configuration

Default The privilege level is 1 by default. Note the default is not shown in running-config output.

Usage notes An intermediate CLI security level (privilege level 7 to privilege level 14) allows a CLI user access to the majority of show commands, including the platform show commands that are available at privilege level 1 to privilege level 6. Note that some show commands, such as **show running-configuration** and **show startup-configuration**, are only available at privilege level 15.

Examples To create the user "bob" with a privilege level of 15, for all show commands including show running-configuration and show startup-configuration and to access configuration commands in Privileged Exec command mode, and the password "bobs_secret", use the commands:

```
awplus# configure terminal
awplus(config)# username bob privilege 15 password bobs_secret
```

To create a user "junior_admin" with a privilege level of 7, which will have intermediate CLI security level access for most show commands, and the password "show_only", use the commands:

```
awplus# configure terminal
awplus(config)# username junior_admin privilege 7 password
show_only
```

Related commands enable password

security-password minimum-categories

security-password minimum-length

5 Subscription Licensing Commands

Introduction

Overview

This chapter provides an alphabetical reference for each of the Subscription Licensing commands.

Subscription Licensing enables you to use Allied Telesis Management Framework (AMF). You need to purchase an AMF subscription for each AMF master or controller node in your AMF network. To see the AMF subscriptions for your device, see the AlliedWare Plus Datasheet.

For step-by-step instructions about how to license AlliedWare Plus devices, see the Licensing Feature Overview and Configuration Guide.

Command List

- "license update file" on page 151
- "license update online" on page 152
- "show license external" on page 153

license update file

Overview Use this command to load a license, after you have manually copied the license file onto the device.

Syntax

```
license update file <filename>
```

Parameter	Description
<filename>	Name and path of the license file on the device.

Mode Privileged Exec

Examples To load a license onto a device from a file called “license_file.lic” that is stored at the top level of Flash memory, use the following command:

```
awplus# license update file license_file.lic
```

Related commands show license external

license update online

Overview From January 2025, this command is no longer available.

To install a subscription license, obtain the license file from your Allied Telesis representative, copy it onto the device, and use the command license update file to load the file.

For step-by-step instructions, see the Licensing Feature Overview and Configuration Guide.

show license external

Overview Use this command to show information about subscription (external) licenses.

Syntax
```
show license external
```

Mode Privileged Exec

Usage notes If you use AMF Recovery to replace a failed device with a new one, you have to transfer the license to the new switch within 28 days. The command output of **show license external** displays a message with instructions for doing this.

Examples To show information about what subscription features the device is licensed for, use the following command:

```
awplus#show license external
```

Related commands license update file

6 System Configuration and Monitoring Commands

Introduction

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

Command List

- "banner display external-manager" on page 156
- "banner exec" on page 157
- "banner external-manager" on page 159
- "banner login (system)" on page 161
- "banner motd" on page 163
- "clock set" on page 165
- "clock summer-time date" on page 166
- "clock summer-time recurring" on page 168
- "clock timezone" on page 170
- "hostname" on page 171
- "low-memory restart" on page 172
- "no debug all" on page 173
- "reboot" on page 175
- "reload" on page 176
- "show banner external-manager" on page 177
- "show clock" on page 178
- "show cpu" on page 180
- "show cpu history" on page 183
- "show debugging" on page 185
- "show interface memory" on page 186

- "show memory" on page 188
- "show memory allocations" on page 190
- "show memory history" on page 192
- "show memory pools" on page 193
- "show memory shared" on page 194
- "show process" on page 195
- "show reboot history" on page 197
- "show router-id" on page 198
- "show system" on page 199
- "show system mac" on page 200
- "show system serialnumber" on page 201
- "show tech-support" on page 202
- "terminal monitor" on page 204
- "undebug all" on page 205

banner display external-manager

Overview Use this command to display the external-manager banner. The external-manager banner warns you that certain features are being managed by an external management system. For example, if you are using Vista Manager EX to manage your network, you will see a notification banner telling you what features are being managed after you enter Global Configuration Mode.

Use the **no** variant of this command to hide the external-manager banner.

Syntax

```
banner display external-manager
no banner display external-manager
```

Default The external-manager banner is displayed by default.

Mode User Exec

Usage notes The external-manager banner is displayed by default. In some instances it is desirable to hide it for the current session. You do this by using the **no** variant of this command. The banner will remain hidden until you either re-enable it, or log out and then log back in.

Example To hide the external-manager banner, use the command:

```
awplus> no banner display external-manager
```

To display the external-manager banner, use the command:

```
awplus> banner display external-manager
```

Related commands banner external-manager

show banner external-manager

Command changes Version 5.5.1-1.1: command added

banner exec

Overview This command configures the User Exec mode banner that is displayed on the console after you login. The **banner exec default** command restores the User Exec banner to the default banner. Use the **no banner exec** command to disable the User Exec banner and remove the default User Exec banner.

Syntax

```
banner exec <banner-text>
banner exec default
no banner exec
```

Default By default, the AlliedWare Plus™ version and build date is displayed at console login, such as:

```
AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00
```

Mode Global Configuration

Examples To configure a User Exec mode banner after login (in this example, to tell people to use the **enable** command to move to Privileged Exec mode), enter the following commands:

```
awplus#configure terminal
awplus(config)#banner exec Use enable to move to Priv Exec mode
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

Use enable to move to Priv Exec mode

awplus>
```

To restore the default User Exec mode banner after login, enter the following commands:

```
awplus#configure terminal
awplus(config)#banner exec default
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00

awplus>
```

To remove the User Exec mode banner after login, enter the following commands:

```
awplus#configure terminal
awplus(config)#no banner exec
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

awplus>
```

Related commands

banner login (system)

banner motd

banner external-manager

Overview Use this command to add an entry to the external-manager banner. The external-manager banner warns you that certain features are being managed by an external management system. For example, if you are using Vista Manager EX to manage your network, you will see a notification banner telling you what features are being managed after you enter Global Configuration Mode.

Use the **no** variant to remove an entry from the external-manager banner.

Syntax

```
banner external-manager <manager-name> feature <feature-name>
note <feature-note>
```

```
no banner external-manager <manager-name> [feature
<feature-name> note <feature-note>]
```

Parameter	Description
<manager-name>	A string that describes the management system.
<feature-name>	A string that describes the feature being managed.
<feature-note>	A note for the feature.

Default No external-manager banner entries are configured by default.

Mode Global Configuration

Usage notes When you run this command:

- if no entry exists for an external manager, the external manager, feature and note are added.
- if an entry already exists for an external manager, the feature and note are added to the existing manager.
- if the feature already exists for that manager, then the note is added to the existing feature.

The **no** variant of this command removes the specified note from the feature of the specified external manager.

- If there are no other notes for the feature, then the feature is removed.
- If the feature is removed and there are no other features for the external manager, then the external manager is removed.

Use the **no** variant with just the external manager name to remove an external manager and all its features and notes.

Example

To add an external manager note for 'Vista Manager' for the feature 'traffic-control' with the note 'Dynamic Traffic Management', use the commands:

```
awplus# configure terminal
awplus(config)# banner external-manager "Vista Manager" feature "traffic-control" note "Dynamic Traffic Management"
```

To remove the external manager note 'Dynamic Traffic Management' from the feature 'traffic-control' of the external manager 'Vista Manager', use the commands:

```
awplus# configure terminal
awplus(config)# no banner external-manager "Vista Manager" feature "traffic-control" note "Dynamic Traffic Management"
```

To remove all external manager features and notes for 'Vista Manager', use the commands:

```
awplus# configure terminal
awplus(config)# no banner external-manager "Vista Manager"
```

Related commands

banner display external-manager

show banner external-manager

Command changes

Version 5.5.1-1.1: command added

banner login (system)

Overview This command configures the login banner that is displayed on the console when you login. The login banner is displayed on all connected terminals. The login banner is displayed after the MOTD (Message-of-the-Day) banner and before the login username and password prompts.

Use the **no banner login** command to disable the login banner.

Syntax

```
banner login
no banner login
```

Default By default, no login banner is displayed at console login.

Mode Global Configuration

Examples To configure a login banner of "Authorised users only" to be displayed when you login, enter the following commands:

```
awplus#configure terminal
awplus(config)#banner login
Type CNTL/D to finish.

Authorised users only

awplus(config)#exit
awplus#exit

Authorised users only

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00

awplus>
```

To remove the login banner, enter the following commands:

```
awplus#configure terminal
awplus(config)#no banner login
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00

awplus>
```

Related commands

banner exec

banner motd

banner motd

Overview Use this command to create or edit the text MotD (Message-of-the-Day) banner displayed before login. The MotD banner is displayed on all connected terminals. The MotD banner is useful for sending messages that affect all network users, for example, any imminent system shutdowns.

Use the **no** variant of this command to delete the MotD banner.

Syntax

```
banner motd <motd-text>
no banner motd
```

Parameter	Description
<motd-text>	The text to appear in the Message of the Day banner.

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

Mode Global Configuration

Examples To configure a MotD banner of "System shutdown at 6pm today" to be displayed when you log in, enter the following commands:

```
awplus>enable
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#banner motd System shutdown at 6pm today
awplus(config)#exit
awplus#exit

System shutdown at 6pm today
awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00

awplus>
```

To delete the login banner, enter the following commands:

```
awplus>enable
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#no banner motd
awplus(config)#exit
awplus#exit

awplus login: manager
Password:

AlliedWare Plus (TM) 5.5.4 04/05/25 12:00:00

awplus>
```

Related commands

banner exec

banner login (system)

clock 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, from 1 to 31
<month>	The first three letters of the current month
<year>	Current year, from 2000 to 2035

Mode Privileged Exec

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

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 October 2016, use the command:

```
awplus# clock set 14:00:00 2 oct 2016
```

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, from 1 to 31.
<start-month>	First three letters of the name of the month that the summertime starts.
<start-year>	Year that summertime starts, from 2000 to 2035.
<start-time>	Time of the day that summertime starts, in the 24-hour time format HH:MM.
<end-day>	Day that summertime ends, from 1 to 31.
<end-month>	First three letters of the name of the month that the summertime ends.
<end-year>	Year that summertime ends, from 2000 to 2035.
<end-time>	Time of the day that summertime ends, in the 24-hour time format HH:MM.
<1-180>	The offset in minutes.

Mode Global Configuration

Examples To set a summertime definition for New Zealand using NZST (UTC+12:00) as the standard time, and NZDT (UTC+13:00) as summertime, with the summertime set to begin on the 25th of September 2016 and end on the 2nd of April 2017:

```
awplus(config)# clock summer-time NZDT date 25 sep 2:00 2016 2
apr 2:00 2017 60
```

To remove any summertime settings on the system, use the command:

```
awplus(config)# no clock summer-time
```

Related commands

clock summer-time recurring

clock timezone

clock summer-time recurring

Overview This command defines the start and end of summertime for every year, and specifies summertime's offset value to Standard Time.

The **no** variant of this command removes the device's summertime setting. This clears both specific summertime dates (set with the clock summer-time date command) and recurring dates.

By default, the device has no summertime definitions set.

Syntax

```
clock summer-time <timezone-name> recurring <start-week>
<start-day> <start-month> <start-time> <end-week> <end-day>
<end-month> <end-time> <1-180>
```

```
no clock summer-time
```

Parameter	Description
<timezone-name>	A description of the summertime zone, up to 6 characters long.
`recurring`	Specifies that this summertime setting applies every year from now on.
<start-week>	Week of the month when summertime starts, in the range 1-5. The value 5 indicates the last week that has the specified day in it for the specified month. For example, to start summertime on the last Sunday of the month, enter 5 for <*start-week*> and sun for <*start-day*>.
<start-day>	Day of the week when summertime starts. Valid values are mon, tue, wed, thu, fri, sat or sun.
<start-month>	First three letters of the name of the month that summertime starts.
<start-time>	Time of the day that summertime starts, in the 24-hour time format HH:MM.
<end-week>	Week of the month when summertime ends, in the range 1-5. The value 5 indicates the last week that has the specified day in it for the specified month. For example, to end summertime on the last Sunday of the month, enter 5 for <*end-week*> and sun for <*end-day*>.
<end-day>	Day of the week when summertime ends. Valid values are mon, tue, wed, thu, fri, sat or sun.
<end-month>	First three letters of the name of the month that summertime ends.
<end-time>	Time of the day that summertime ends, in the 24-hour time format HH:MM.
<1-180>	The offset in minutes.

Mode Global Configuration

Examples To set a summertime definition for New Zealand using NZST (UTC+12:00) as the standard time, and NZDT (UTC+13:00) as summertime, with summertime set to start on the last Sunday in September, and end on the 1st Sunday in April, use the command:

```
awplus(config)# clock summer-time NZDT recurring 5 sun sep 2:00
1 sun apr 2:00 60
```

To remove any summertime settings on the system, use the command:

```
awplus(config)# no clock summer-time
```

Related commands clock summer-time date

clock timezone

clock timezone

Overview This command defines the device's clock timezone. The timezone is set as a offset to the UTC.

The **no** variant of this command resets the system time to UTC.

By default, the system time is set to UTC.

Syntax

```
clock timezone <timezone-name> {minus|plus}
[<0-13>|<0-12>:<00-59>]
no clock timezone
```

Parameter	Description
<timezone-name>	A description of the timezone, up to 6 characters long.
minusorplus	The direction of offset from UTC. The **minus** option indicates that the timezone is behind UTC. The **plus** option indicates that the timezone is ahead of UTC.
<0-13>	The offset in hours or from UTC.
<0-12>:<00-59>	The offset in hours or from UTC.

Mode Global Configuration

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

Examples To set the timezone to New Zealand Standard Time with an offset from UTC of +12 hours, use the command:

```
awplus(config)# clock timezone NZST plus 12
```

To set the timezone to Indian Standard Time with an offset from UTC of +5:30 hours, use the command:

```
awplus(config)# clock timezone IST plus 5:30
```

To set the timezone back to UTC with no offsets, use the command:

```
awplus(config)# no clock timezone
```

Related commands

clock set

clock summer-time date

clock summer-time recurring

hostname

Overview This command sets the name applied to the device as shown at the prompt. The hostname is:

- displayed in the output of the show system command
- displayed in the CLI prompt so you know which device you are configuring
- stored in the MIB object sysName

Use the **no** variant of this command to revert the hostname setting to its default. For devices that are not part of an AMF network, the default is "awplus".

Syntax

```
hostname <hostname>
no hostname [<hostname>]
```

Parameter	Description
<hostname>	Specifies the name given to a specific device.

Default `awplus`

Mode Global Configuration

Usage notes Within an AMF network, any device without a user-defined hostname will automatically be assigned a name based on its MAC address.

To efficiently manage your network using AMF, we strongly advise that you devise a naming convention for your network devices and apply an appropriate hostname to each device.

The name must also follow the rules for ARPANET host names. The name must start with a letter, end with a letter or digit, and use only letters, digits, and hyphens. Refer to RFC 1035.

Example To set the system name to `HQ-Sales`, use the command:

```
awplus# configure terminal
awplus(config)# hostname HQ-Sales
```

This changes the prompt to:

```
HQ-Sales(config)#
```

To revert to the default hostname `awplus`, use the command:

```
HQ-Sales(config)# no hostname
```

This changes the prompt to:

```
awplus(config)#
```

Related commands show system

low-memory restart

Overview Use this command to specify a process for the device to terminate if available memory is sufficiently low.

This command is intended for use in consultation with Allied Telesis customer support. Using this command will make the device produce a core dump when the process terminates, which makes it easier for Allied Telesis engineers to debug any issues.

Use the **no** variant of this command to stop specifying the process for termination.

Syntax

```
low-memory restart <process-name>
no low-memory restart <process-name>
```

Parameter	Description
<process-name>	The name of a process to terminate if the device memory gets sufficiently low.

Default None. By default, the device will automatically terminate the non-critical process that has the highest memory consumption. Note that only a non-critical process will be terminated automatically, not a critical process.

Mode Global Configuration

Usage notes The process does not have to be running when you enter this command. If it is running at the time the available memory becomes sufficiently low, the device will terminate it.

Example To specify RIP as the process to terminate if memory gets too low, use the commands:

```
awplus# configure terminal
awplus(config)# low-memory restart ripd
```

Related commands show memory

snmp-server enable trap

Command changes Version 5.5.4-2.3: command added

no debug all

Overview This command disables the debugging facility for all features on your device. This stops the device from generating any diagnostic debugging messages.

You can optionally disable the debugging facility for only the given protocol or feature. The features available depend on your device and will be a subset of the features listed in the Syntax section below.

Syntax

```
no debug all [bgp|ipv6 ospf|ipv6 rip|dot1x|nsm|ospf|pim
dense-mode|pim sparse-mode|rip|vrrp]
```

Parameter	Description
`bgp`	Turns off all debugging for BGP (Border Gateway Protocol).
`dot1x`	Turns off all debugging for IEEE 802.1X port-based network access- control.
`ipv6 ospf`	Turns off all debugging for IPv6 OSPF (Open Shortest Path First).
`ipv6 rip`	Turns off all debugging for IPv6 RIP (Routing Information Protocol).
`nsm`	Turns off all debugging for the NSM (Network Services Module).
`ospf`	Turns off all debugging for OSPF (Open Shortest Path First).
`pim dense-mode`	Turns off all debugging for PIM (Protocol Independent Multicast) Dense Mode.
`pim sparse-mode`	Turns off all debugging for PIM (Protocol Independent Multicast) Sparse Mode.
`rip`	Turns off all debugging for RIP (Routing Information Protocol).
`vrrp`	Turns off all debugging for VRRP (Virtual Router Redundancy Protocol).

Default Disabled

Mode Global Configuration and Privileged Exec

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

```
awplus# no debug all
```

To disable all NSM debugging, use the command:

```
awplus# no debug all nsm
```

Related commands undebug all

Command changes Version 5.4.7-1.1: **pim dense-mode**, **pim sparse-mode**, and **rip** parameters added

reboot

Overview This command halts the device and performs a cold restart (also known as reload). It displays a confirmation request before restarting.

Syntax

```
reboot
reload
```

Mode Privileged Exec

Usage notes The **reboot** and **reload** commands perform the same action.

Examples To restart the device, use the command:

```
awplus# reboot
reboot system? (y/n): y
```

reload

Overview This command performs the same function as the reboot command.

show banner external-manager

Overview Use this command to show the current external-manager banner. The external-manager banner warns you that certain features are being managed by an external management system. For example, if you are using Vista Manager EX to manage your network, you will see a notification banner telling you which features are being managed after you enter Global Configuration Mode.

Syntax

```
show banner external-manager
```

Mode User Exec

Example To show the external-manager banner, use the command:

```
awplus# show banner external-manager
```

Output Figure 6-1: Example output from **show banner external-manager**

```
awplus#show banner external-manager
The following features are being managed by external systems.
Configuring these features may have unintended consequences.
Manager: Network Manager
  Feature: ACLs
    Filters

Manager: Vista Manager
  Feature: Traffic control
    Application Priority
    Dynamic Traffic Management
  Feature: Web control
    all features
```

Related commands banner display external-manager

banner external-manager

Command changes Version 5.5.1-1.1: command added

show clock

Overview This command displays the system's current configured local time and date. It also displays other clock related information such as timezone and summertime configuration.

Syntax

```
show clock
```

Mode User Exec and Privileged Exec

Example To display the system's current local time, use the command:

```
awplus# show clock
```

Output Figure 6-2: Example output from the **show clock** command for a device using New Zealand time

```
Local Time: Mon,  17 Oct 2016 13:56:06 +1200
UTC Time:   Mon,  17 Oct 2016 01:56:06 +0000
Timezone: NZST
Timezone Offset: +12:00
Summer time zone: NZDT
Summer time starts: Last Sunday in September at 02:00:00
Summer time ends: First Sunday in April at 02:00:00
Summer time offset: 60 mins
Summer time recurring: Yes
```

Table 1: Parameters in the output of the **show clock** command

Parameter	Description
Local Time	Current local time.
UTC Time	Current UTC time.
Timezone	The current configured timezone name.
Timezone Offset	Number of hours offset to UTC.
Summer time zone	The current configured summertime zone name.
Summer time starts	Date and time set as the start of summer time.
Summer time ends	Date and time set as the end of summer time.
Summer time offset	Number of minutes that summer time is offset from the system's timezone.
Summer time recurring	Whether the device will apply the summer time settings every year or only once.

Related commands

clock set

clock summer-time date

clock summer-time recurring

clock timezone

show cpu

Overview This command displays a list of running processes with their CPU utilization.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show cpu [sort {thrds|pri|sleep|runtime}]
```

Parameter	Description	
`sort`	Changes the sorting order using the following fields. If you do not specify a field, then the list is sorted by percentage CPU utilization.	
	`thrds`	Sort by the number of threads.
	`pri`	Sort by the process priority.
	`sleep`	Sort by the average time sleeping.
	`runtime`	Sort by the runtime of the process.

Mode User Exec and Privileged Exec

Examples To show the CPU utilization of current processes, sorting them by the number of threads the processes are using, use the command:

```
awplus# show cpu sort thrds
```

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

```
CPU averages:
 1 second: 12%, 20 seconds: 2%, 60 seconds: 2%
System load averages:
 1 minute: 0.03, 5 minutes: 0.02, 15 minutes: 0.00
Current CPU load:
 userspace: 6%, kernel: 4%, interrupts: 1% iowaits: 0%

user processes
==============
  pid name            thrds  cpu%   pri state sleep% runtime
 1544 hostd              1   2.8    20   run     0   120
 1166 exfx              17   1.8    20 sleep     0  3846
 1284 aisexec           44   0.9    -2 sleep     0  2606
    1 init               1   0.0    20 sleep     0   120
 9772 sh                 1   0.0    20 sleep     0     0
 9773 corerotate         1   0.0    20 sleep     0     0
  853 syslog-ng          1   0.0    20 sleep     0   356
  859 klogd              1   0.0    20 sleep     0     1
  910 inetd              1   0.0    20 sleep     0     3
  920 portmap            1   0.0    20 sleep     0     0
  931 crond              1   0.0    20 sleep     0     1
 1090 openhpid          11   0.0    20 sleep     0   233
 1111 hpilogd            1   0.0    20 sleep     0     0
 1240 hsl                1   0.0    20 sleep     0    79
 1453 authd              1   0.0    20 sleep     0    85
 ...
```

Table 2: Parameters in the output of the **show cpu** command

Parameter	Description
`CPU averages`	Average CPU utilization for the periods stated.
`System load averages`	The average number of processes waiting for CPU time for the periods stated.
`Current CPU load`	Current CPU utilization specified by load types.
`pid`	Identifier number of the process.
`name`	A shortened name for the process
`thrds`	Number of threads in the process.
`cpu%`	Percentage of CPU utilization that this process is consuming.
`pri`	Process priority state.
`state`	Process state; one of “run”, “sleep”, “zombie”, and “dead”.

Table 2: Parameters in the output of the **show cpu** command (cont.)

Parameter	Description
`sleep%`	Percentage of time that the process is in the sleep state.
`runtime`	The time that the process has been running for, measured in jiffies. A jiffy is the duration of one tick of the system timer interrupt.

Related commands

show memory

show memory allocations

show memory history

show memory pools

show process

show cpu history

Overview This command prints a graph showing the historical CPU utilization.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show cpu history
```

Mode User Exec and Privileged Exec

Usage notes This command's output displays three graphs of the percentage CPU utilization:

- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

Examples To display a graph showing the historical CPU utilization of the device, use the command:

```
awplus# show cpu history
```

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

```
Per second CPU load history

100
 90
 80
 70
 60
 50
 40
 30
 20                                          *
 10 ******************************************* ***************
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                 Newest
        CPU load% per second (last 60 seconds)
              * = average CPU load%
```

```
Per minute CPU load history

100
 90
 80
 70
 60                                                  +
 50
 40
 30
 20 ++ +++++++++ +++++++ ++++ + ++++++ ++++ +++ +++++ +++++++++
 10 ************************************************************
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                 Newest
        CPU load% per minute (last 60 minutes)
              * = average CPU load%, + = maximum

Per (30) minute CPU load history

100
 90
 80
 70                                                        +
 60
 50
 40
 30
 20
 10                                                       ***
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                 Newest
        CPU load% per 30 minutes (last 60 values / 30 hours)
              * = average, - = minimum, + = maximum
```

Related commands

show memory

show memory allocations

show memory pools

show process

show debugging

Overview This command displays all debugging options in alphabetical order, indicating whether debugging is enabled or disabled for each feature.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging
```

Mode User Exec and Privileged Exec

Example To find out what debugging is enabled, use the command:

```
awplus# show debugging
```

Output Figure 6-5: 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 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 the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show interface memory
show interface <port-list> memory
```

Parameter	Description
<port-list>	Display information about only the specified port or ports. The port list can be: • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the **encapsulation dot1q** command). Ranges of sub-interfaces are not supported. • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list.

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 eth0, use the command:

```
awplus# show interface eth0 memory
```

Output Figure 6-6: Example output from the **show interface memory** command

```
awplus#show interface memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
eth0         393228       512            1
lo           425997       512            1
br1          557073       512            1
```

Figure 6-7: Example output from **show interface <port-list> memory** for a list of interfaces

```
awplus#show interface eth0 memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
eth0         393228       512            1
```

Related commands

show interface brief

show interface status

show memory

Overview This command displays the memory used by each process that is currently running.

For information on filtering and saving command output, see the Getting Started with the AlliedWare Plus Command Line Interface.

Syntax

```
show memory [sort {size|peak|stk}]
```

Parameter	Description	
`sort`	Changes the sorting order for the list of processes. If you do not specify this, then the list is sorted by percentage memory utilization.	
	`size`	Sort by the amount of memory the process is currently using.
	`peak`	Sort by the greatest amount of memory ever used by the process.
	`stk`	Sort by the stack size of the process.

Mode User Exec and Privileged Exec

Example To display the memory used by the current running processes, use the command:

```
awplus# show memory
```

Output Figure 6-8: Example output from **show memory**

```
awplus#show memory

RAM total: 1014200 kB; free: 818320 kB; buffers: 25788 kB

user processes
==============
  pid name             mem%  size(kB)  peak(kB)  data(kB)   stk(kB)  virt(kB)
 1443 appweb            1.6     16480    830728    455528       136    765192
  899 imi               1.4     14896   5893624   5523944       136   5836384
  895 nsm               1.2     12620   5618080   5318380       136   5552544
127767 imish            1.1     11368   4617296   4417068       136   4617296
 1829 imish             1.1     11424   4608968   4343204       136   4543432
  960 atmfd             0.9      9920   5205744   4940732       136   5140448
  907 hsl               0.9      9324   4576324   4342560       136   4510788
 1790 lua               0.8      8192    453184    297316       136    387736
 1128 snmpd             0.7      8016     77020      1480       340     77020
...
```

Table 3: Parameters in the output of the **show memory** command

Parameter	Description
`RAM total`	Total amount of RAM memory free.
`free`	Available memory size.
`buffers`	Memory allocated kernel buffers.
`pid`	Identifier number for the process.
`name`	Short name used to describe the process.
`mem%`	Percentage of memory utilization the process is currently using.
`size`	Amount of memory currently used by the process.
`peak`	Greatest amount of memory ever used by the process.
`data`	Amount of memory used for data.
`stk`	The stack size.

Related commands

low-memory restart

show memory allocations

show memory history

show memory pools

show memory shared

snmp-server enable trap low-memory

show memory allocations

Overview This command displays the memory allocations used by processes.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show memory allocations [<process>]
```

Parameter	Description
<process>	Displays the memory allocation used by the specified process.

Mode User Exec and Privileged Exec

Example To display the memory allocations used by all processes on your device, use the command:

```
awplus# show memory allocations
```

Output Figure 6-9: Example output from the **show memory allocations** command

```
awplus#show memory allocations
Memory allocations for imi
----------------------------

Current 15093760 (peak 15093760)

Statically allocated memory:
 - binary/exe                :    1675264
 - libraries                 :    8916992
 - bss/global data           :    2985984
 - stack                     :     139264

Dynamically allocated memory (heap):
 - total allocated           :    1351680
   - in use                  :    1282440
   - non-mmapped             :    1351680
 - maximum total allocated   :    1351680
 - total free space          :      69240
   - releasable              :      68968
   - space in freed fastbins :         16

Context
           filename:line   allocated      freed
 +            lib.c:749          484
.
.
.
```

Related commands

show memory

show memory history

show memory pools

show memory shared

show tech-support

show memory history

Overview This command prints a graph showing the historical memory usage.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show memory history
```

Mode User Exec and Privileged Exec

Usage notes This command's output displays three graphs of the percentage memory utilization:

- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

Examples To show a graph displaying the historical memory usage, use the command:

```
awplus# show memory history
```

Output Figure 6-10: Example output from the **show memory history** command

Related commands

show memory allocations

show memory pools

show memory shared

show tech-support

show memory pools

Overview This command shows the memory pools used by processes.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show memory pools [<process>]
```

Parameter	Description
<process>	Displays the memory pools used by the specified process.

Mode User Exec and Privileged Exec

Example To shows the memory pools used by processes, use the command:

```
awplus# show memory pools
```

Output Figure 6-11: Example output from the **show memory pools** command

```
awplus#show memory pools
Memory pools for imi
----------------------

Current 15290368 (peak 15290368)

Statically allocated memory:
 - binary/exe                 :    1675264
 - libraries                  :    8916992
 - bss/global data            :    2985984
 - stack                      :     139264

Dynamically allocated memory (heap):
 - total allocated            :    1548288
   - in use                   :    1479816
   - non-mmapped              :    1548288
 - maximum total allocated    :    1548288
 - total free space           :      68472
   - releasable               :      68200
   - space in freed fastbins  :         16
.
.
.
```

Related commands

show memory allocations

show memory history

show tech-support

show memory shared

Overview This command displays shared memory allocation information. The output is useful for diagnostic purposes by Allied Telesis authorized service personnel.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show memory shared
```

Mode User Exec and Privileged Exec

Example To display information about the shared memory allocation used on the device, use the command:

```
awplus# show memory shared
```

Output Figure 6-12: Example output from the **show memory shared** command

```
awplus#show memory shared
Shared Memory Status
--------------------------
Segment allocated  = 39
Pages allocated    = 39
Pages resident     = 11

Shared Memory Limits
--------------------------
Maximum number of segments          = 4096
Maximum segment size (kbytes)       = 32768
Maximum total shared memory (pages) = 2097152
Minimum segment size (bytes)        = 1
```

Related commands

show memory allocations

show memory history

show memory

show process

Overview This command lists a summary of the current running processes.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show process [sort {cpu|mem}]
```

Parameter	Description	
sort	Changes the sorting order for the list of processes.	
	cpu	Sorts the list by the percentage of CPU utilization.
	mem	Sorts the list by the percentage of memory utilization.

Mode User Exec and Privileged Exec

Usage notes This command displays a snapshot of currently-running processes. If you want to see CPU or memory utilization history instead, use the commands show cpu history or show memory history.

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

```
awplus# show process
```

Output Figure 6-13: Example output from the **show process** command

```
CPU averages:
 1 second: 8%, 20 seconds: 5%, 60 seconds: 5%
System load averages:
 1 minute: 0.04, 5 minutes: 0.08, 15 minutes: 0.12
Current CPU load:
 userspace: 9%, kernel: 9%, interrupts: 0% iowaits: 0%
RAM total: 514920 kB; free: 382600 kB; buffers: 16368 kB

user processes
==============
pid name          thrds  cpu%  mem%   pri  state  sleep%
962 pss             12     0     6    25  sleep       5
1   init             1     0     0    25  sleep       0
797 syslog-ng        1     0     0    16  sleep      88
...
kernel threads
==============
pid name          cpu%  pri  state  sleep%
71  aio/0         0     20   sleep  0
3   events/0      0     10   sleep  98
...
```

Table 4: Parameters in the output from the **show process** command

Parameter	Description
`CPU averages`	Average CPU utilization for the periods stated.
`System load averages`	The average number of processes waiting for CPU time for the periods stated.
`Current CPU load`	Current CPU utilization specified by load types
`RAM total`	Total memory size.
`free`	Available memory.
`buffers`	Memory allocated to kernel buffers.
`pid`	Identifier for the process.
`name`	Short name to describe the process.
`thrds`	Number of threads in the process.
`cpu%`	Percentage of CPU utilization that this process is consuming.
`mem%`	Percentage of memory utilization that this process is consuming.
`pri`	Process priority.
`state`	Process state; one of “run”, “sleep”, “stop”, “zombie”, or “dead”.
`sleep%`	Percentage of time the process is in the sleep state.

Related commands

show cpu

show cpu history

show reboot history

Overview Use this command to display the device's reboot history.

Syntax

```
show reboot history
```

Mode User Exec and Privileged Exec

Example To show the reboot history, use the command:

```
awplus# show reboot history
```

Output Figure 6-14: Example output from the **show reboot history** command

```
awplus#show reboot history

<date>     <time>    <type>      <description>
-----------------------------------------------
2016-10-10 01:42:04  Expected    User Request
2016-10-10 01:35:31  Expected    User Request
2016-10-10 01:16:25  Unexpected  Rebooting due to critical process (network/nsm)
failure!
2016-10-10 01:11:04  Unexpected  Rebooting due to critical process (network/nsm)
failure!
2016-10-09 19:56:16  Expected    User Request
2016-10-09 19:51:20  Expected    User Request
```

Table 5: Parameters in the output from the **show reboot history** command

Parameter	Description
Unexpected	A non-intended reboot.
Expected	A planned or user-triggered reboot.
User request	User initiated reboot via the CLI.

Related commands show tech-support

show router-id

Overview Use this command to show the Router ID of the current system.

Syntax

```
show router-id
```

Mode User Exec and Privileged Exec

Example To display the Router ID of the current system, use the command:

```
awplus# show router-id
```

Output Figure 6-15: Example output from the **show router-id** command

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

show system

Overview Use this command to display general system information about the device, including the hardware, memory usage, and software version. It also displays location and contact details when these have been set.

For information on filtering and saving command output, see the Getting Started with the AlliedWare Plus Command Line Interface.

Syntax

```
show system
```

Mode User Exec and Privileged Exec

Example To display configuration information, use the command:

```
awplus# show system
```

Output Figure 6-16: Example output from **show system**

```
awplus#show system
System Status                                        Thu Jun 25 10:32:16 2020

Board      ID   Bay     Board Name                      Rev   Serial number
-------------------------------------------------------------------------------
Base       441  Base    AT-VAA                          A-0   V3E6E1E4D84393DE
-------------------------------------------------------------------------------
RAM: Total: 1014200 kB Free: 817692 kB
Flash: 4.6GB Used: 290.9MB Available: 4.0GB
-------------------------------------------------------------------------------
Uptime             : 6 days 19:27:25

Current software   : vaa-5.5.0-0.3.iso
Software version   : 5.5.0-0.3
Build date         : Thu Jun 4 07:03:29 UTC 2020

Current boot config: flash:/default.cfg (file exists)

System Name
 awplus
System Contact
System Location
-------------------------------------------------------------------------------
```

show system mac

Overview This command displays the physical MAC address of the device.

Syntax

```
show system mac
```

Mode User Exec and Privileged Exec

Example To display the physical MAC address enter the following command:

```
awplus# show system mac
```

Output Figure 6-17: Example output from the **show system mac** command

```
awplus#show system mac
0200.0034.5682 (eth0)
0200.0034.5683 (system)
```

show system serialnumber

Overview This command shows the serial number information for the device.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show system serialnumber
```

Mode User Exec and Privileged Exec

Example To display the serial number information for the device, use the command:

```
awplus# show system serialnumber
```

Output Figure 6-18: Example output from the **show system serialnumber** command

```
awplus#show system serialnumber
45AX5300X
```

show tech-support

Overview This command generates system and debugging information for the device and saves it to a file.

This command is useful for collecting a large amount of information so that it can then be analyzed for troubleshooting purposes. The output of this command can be provided to technical support staff when reporting a problem.

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

Syntax

```
show tech-support
{[all|atmf|auth|bgp|card|dhcpsn|epsr|firewall|igmp|ip|ipv6|mld
|openflow|ospf|ospf6|pim|rip|ripng|stack|stp|system|tacacs+|
update]} [outfile <filename>]
```

Parameter	Description
`all`	Display full information
`atmf`	Display ATMF-specific information
`auth`	Display authentication-related information
`bgp`	Display BGP-related information
`card`	Display Chassis Card specific information
`dhcpsn`	Display DHCP Snooping specific information
`epsr`	Display EPSR specific information
`firewall`	Display firewall specific information
`igmp`	Display IGMP specific information
`ip`	Display IP specific information
`ipv6`	Display IPv6 specific information
`mld`	Display MLD specific information
`openflow`	Display information related to OpenFlow
`ospf`	Display OSPF related information
`ospf6`	Display OSPF6 specific information
`pim`	Display PIM related information
`rip`	RIP related information
`ripng`	Display RIPNG specific information
`stack`	Display stacking device information
`stp`	Display STP specific information
`system`	Display general system information

Parameter	Description
`tacacs+`	Display TACACS+ information
`update`	Display resource update specific information
`|`	Output modifier
`>`	Output redirection
`>>`	Output redirection (append)
`outfile`	Output file name
`<filename>`	Specifies a name for the output file. If no name is specified, this file will be saved as: tech-support.txt.gz.

Default Captures **all** information for the device.

By default the output is saved to the file 'tech-support.txt.gz' in the current directory. If this file already exists in the current directory then a new file is generated with the time stamp appended to the file name, for example 'tech-support20161009.txt.gz', so the previous file is retained.

Usage notes The command generates a large amount of output, which is saved to a file in compressed format. The output file name can be specified by outfile option. If the output file already exists, a new file name is generated with the current time stamp. If the output filename does not end with ".gz", then ".gz" is appended to the filename. Since output files may be too large for Flash on the device we recommend saving files to external memory or a TFTP server whenever possible to avoid device lockup. This method is not likely to be appropriate when running the working set option of AMF across a range of physically separated devices.

Mode Privileged Exec

Examples To produce the output needed by technical support staff, use the command:

```
awplus# show tech-support
```

terminal monitor

Overview Use this command to display debugging output on a terminal.

To display the cursor after a line of debugging output, press the Enter key.

Use the command **terminal no monitor** or **no terminal monitor** to stop displaying debugging output on the terminal. Alternatively, you can use the timeout option to stop displaying debugging output on the terminal after a set time.

Syntax

```
terminal monitor [<1-60>]
terminal no monitor
no terminal monitor
```

Parameter	Description
<1-60>	Set a timeout between 1 and 60 seconds for terminal output.

Default Disabled

Mode User Exec and Privileged Exec

Examples To display debugging output on a terminal, enter the command:

```
awplus# terminal monitor
```

To display debugging on the terminal for 60 seconds, enter the command:

```
awplus# terminal monitor 60
```

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

```
awplus# no terminal monitor
```

Related commands All debug commands

Command changes Version 5.4.8-0.2: **no terminal monitor** added as an alias for **terminal no monitor**

undebug all

Overview This command applies the functionality of the no debug all command.

7 Logging Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure logging. See the Logging Feature Overview and Configuration Guide for more information about the different types of log and how to filter log messages.

Command List

- "clear exception log" on page 208
- "clear log" on page 209
- "clear log buffered" on page 210
- "clear log permanent" on page 211
- "copy buffered-log" on page 212
- "copy permanent-log" on page 213
- "default log buffered" on page 214
- "default log console" on page 215
- "default log email" on page 216
- "default log host" on page 217
- "default log monitor" on page 218
- "default log permanent" on page 219
- "log buffered" on page 220
- "log buffered (filter)" on page 221
- "log buffered exclude" on page 224
- "log buffered size" on page 227
- "log console" on page 228
- "log console (filter)" on page 229
- "log console exclude" on page 232

- "log email" on page 235
- "log email (filter)" on page 236
- "log email exclude" on page 239
- "log email time" on page 242
- "log facility" on page 244
- "log host" on page 246
- "log host (filter)" on page 248
- "log host exclude" on page 251
- "log host source" on page 254
- "log host startup-delay" on page 255
- "log host time" on page 257
- "log monitor (filter)" on page 259
- "log monitor exclude" on page 262
- "log permanent" on page 265
- "log permanent (filter)" on page 266
- "log permanent exclude" on page 269
- "log permanent size" on page 272
- "log-rate-limit nsm" on page 273
- "log trustpoint" on page 274
- "show counter log" on page 275
- "show exception log" on page 276
- "show log" on page 277
- "show log config" on page 279
- "show log permanent" on page 281
- "show running-config log" on page 283

clear exception log

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

Syntax
```
clear exception log
```

Mode Privileged Exec

Example
```
awplus# clear exception log
```

clear log

Overview This command removes the contents of the buffered and permanent logs.

Syntax

```
clear log
```

Mode Privileged Exec

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

```
awplus# clear log
```

Related commands

clear log buffered

clear log permanent

show log

clear log buffered

Overview This command removes the contents of the buffered log.

Syntax

```
clear log buffered
```

Mode Privileged Exec

Example To delete the contents of the buffered log use the following commands:

```
awplus# clear log buffered
```

Related commands

default log buffered

log buffered

log buffered (filter)

log buffered size

log buffered exclude

show log

show log config

clear log permanent

Overview This command removes the contents of the permanent log.

Syntax

```
clear log permanent
```

Mode Privileged Exec

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

```
awplus# clear log permanent
```

Related commands

default log permanent

log permanent

log permanent (filter)

log permanent exclude

log permanent size

show log config

show log permanent

copy buffered-log

Overview Use this command to copy the buffered log to an internal or external destination.

Syntax

```
copy buffered-log <destination-name>
```

Parameter	Description
<destination-name>	The filename and path for the destination file. See Introduction on page 64 for valid syntax.

Mode Privileged Exec

Example To copy the buffered log file into a folder in Flash named "buffered-log" and name the file "buffered-log.log", use the command:

```
awplus# copy buffered-log flash:/buffered-log/buffered-log.log
```

Related commands

log buffered

show file systems

show log

Command changes Version 5.4.7-1.1: command added

copy permanent-log

Overview Use this command to copy the permanent log to an internal or external destination.

Syntax

```
copy permanent-log <destination-name>
```

Parameter	Description
<destination-name>	The filename and path for the destination file. See Introduction on page 64 for valid syntax.

Mode Privileged Exec

Example To copy the permanent log file into a folder in Flash named "perm-log" and name the file "permanent-log.log", use the command:

```
awplus# copy permanent-log flash:/perm-log/permanent-log.log
```

Related commands

log permanent

show file systems

show log permanent

Command changes Version 5.4.7-1.1: command added

default log buffered

Overview This command restores the default settings for the buffered log stored in RAM. By default the size of the buffered log is 50 kB and it accepts messages with the severity level of “warnings” and above.

Syntax

```
default log buffered
```

Default The buffered log is enabled by default.

Mode Global Configuration

Example To restore the buffered log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log buffered
```

Related commands

clear log buffered

log buffered

log buffered (filter)

log buffered size

log buffered exclude

show log

show log config

default log console

Overview This command restores the default settings for log messages sent to the terminal when a log console command is issued. By default all messages are sent to the console when a **log console** command is issued.

Syntax

```
default log console
```

Mode Global Configuration

Example To restore the log console to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log console
```

Related commands

log console

log console (filter)

log console exclude

show log config

default log email

Overview This command restores the default settings for log messages sent to an email address. By default no filters are defined for email addresses. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax

```
default log email <email-address>
```

Parameter	Description
<email-address>	The email address to send log messages to

Mode Global Configuration

Example To restore the default settings for log messages sent to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# default log email admin@alliedtelesis.com
```

Related commands

log email

log email (filter)

log email exclude

log email time

show log config

default log host

Overview This command restores the default settings for log sent to a remote syslog server. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax

```
default log host <ip-addr>
```

Parameter	Description
<ip-addr>	The IP address of a remote syslog server

Mode Global Configuration

Example To restore the default settings for messages sent to the remote syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# default log host 10.32.16.21
```

Related commands

log host

log host (filter)

log host exclude

log host source

log host time

show log config

default log monitor

Overview This command restores the default settings for log messages sent to the terminal when a terminal monitor command is used.

Syntax

```
default log monitor
```

Default All messages are sent to the terminal when a terminal monitor command is used.

Mode Global Configuration

Example To restore the log monitor to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log monitor
```

Related commands

log monitor (filter)

log monitor exclude

show log config

terminal monitor

default log permanent

Overview This command restores the default settings for the permanent log stored in NVS. By default, the size of the permanent log is 50 kB and it accepts messages with the severity level of `warnings` and above.

Syntax
```
default log permanent
```

Default The permanent log is enabled by default.

Mode Global Configuration

Example To restore the permanent log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log permanent
```

Related commands
clear log permanent
log permanent
log permanent (filter)
log permanent exclude
log permanent size
show log config
show log permanent

log buffered

Overview This command configures the device to store log messages in RAM. Messages stored in RAM are not retained on the device over a restart. Once the buffered log reaches its configured maximum allowable size old messages will be deleted to make way for new ones.

Syntax

```
log buffered
no log buffered
```

Default The buffered log is configured by default.

Mode Global Configuration

Examples To configured the device to store log messages in RAM use the following commands:

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

To configure the device to not store log messages in a RAM buffer use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered
```

Related commands

clear log buffered

copy buffered-log

default log buffered

log buffered (filter)

log buffered size

log buffered exclude

show log

show log config

log buffered (filter)

Overview Use this command to create a filter to select messages to be sent to the buffered log. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the buffered log.

Syntax

```
log buffered [level <level>] [program <program-name>] [facility
<facility>] [msgtext <text-string>]

no log buffered [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Filter messages to the buffered log by severity level.	
<level>	The minimum severity of message to send to the buffered log. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages to the buffered log by program. Include messages from a specified program in the buffered log.	
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)
	`bgp`	Border Gateway Protocol (BGP)
	`rsvp`	Resource Reservation Protocol (RSVP)
	`pim-dm`	Protocol Independent Multicast - Dense Mode (PIM-DM)

Parameter	Description	
	`pim-sm`	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	`pim-smv6`	PIM-SM version 6 (PIM-SMv6)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`irdp`	ICMP Router Discovery Protocol (IRDP)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Filter messages to the buffered log by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from in the buffered log:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Select messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default By default the buffered log has a filter to select messages whose severity level is "notices (5)" or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To add a filter to send all messages containing the text "Bridging initialization" to the buffered log, use the following commands:

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

To remove a filter that sends all messages containing the text "Bridging initialization" to the buffered log, use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered msgtext Bridging initialization
```

Related commands

clear log buffered

default log buffered

log buffered

log buffered size

log buffered exclude

show log

show log config

log buffered exclude

Overview Use this command to exclude specified log messages from the buffered log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log buffered exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log buffered exclude [level <level>] [program
<program-name>] [facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)
	`bgp`	Border Gateway Protocol (BGP)

Parameter	Description	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`pim-dm`	Protocol Independent Multicast - Dense Mode (PIM-DM)
	`pim-sm`	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	`pim-smv6`	PIM-SM version 6 (PIM-SMv6)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`irdp`	ICMP Router Discovery Protocol (IRDP)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Exclude messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered exclude msgtext example of
irrelevant message
```

Related commands

clear log buffered

default log buffered

log buffered

log buffered (filter)

log buffered size

show log

show log config

log buffered size

Overview This command configures the amount of memory that the buffered log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

Use the **no** variant of this command to return to the default.

Syntax

```
log buffered size <50-250>
no log buffered size
```

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

Default 50 kilobytes

Mode Global Configuration

Example To allow the buffered log to use up to 100 kilobytes of RAM, use the commands:

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

To return to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no log buffered size
```

Related commands

clear log buffered

copy buffered-log

default log buffered

log buffered

log buffered (filter)

log buffered exclude

show log

show log config

log console

Overview This command configures the device to send log messages to consoles. The console log is configured by default to send messages to the device's main console port.

Use the **no** variant of this command to configure the device not to send log messages to consoles.

Syntax

```
log console
no log console
```

Mode Global Configuration

Examples To configure the device to send log messages use the following commands:

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

To configure the device not to send log messages in all consoles use the following commands:

```
awplus# configure terminal
awplus(config)# no log console
```

Related commands

default log console

log console (filter)

log console exclude

show log config

log console (filter)

Overview This command creates a filter to select messages to be sent to all consoles when the **log console** command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

Syntax

```
log console [level <level>] [program <program-name>] [facility
<facility>] [msgtext <text-string>]
```

```
no log console [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Filter messages by severity level.	
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages by program. Include messages from a specified program.	
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)
	`bgp`	Border Gateway Protocol (BGP)
	`rsvp`	Resource Reservation Protocol (RSVP)
	`pim-dm`	Protocol Independent Multicast - Dense Mode (PIM-DM)
	`pim-sm`	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	`pim-smv6`	PIM-SM version 6 (PIM-SMv6)

Parameter	Description	
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`irdp`	ICMP Router Discovery Protocol (IRDP)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Filter messages by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Select messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default By default the console log has a filter to select messages whose severity level is `critical` or higher. This filter may be removed using the **no** variant of this command. This filter may be removed and replaced by filters that are more selective.

Mode Global Configuration

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

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

To remove a default filter that includes sending **critical**, **alert** and **emergency** level messages to the console, use the following commands:

```
awplus# configure terminal
awplus(config)# no log console level critical
```

Related commands

default log console

log console

log console exclude

show log config

log console exclude

Overview Use this command to prevent specified log messages from being sent to the console, when console logging is turned on. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)

Parameter	Description	
	bgp	Border Gateway Protocol (BGP)
	rsvp	Resource Reservation Protocol (RSVP)
	pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
	pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	pim-smv6	PIM-SM version 6 (PIM-SMv6)
	dot1x	IEEE 802.1X Port-Based Access Control
	lacp	Link Aggregation Control Protocol (LACP)
	stp	Spanning Tree Protocol (STP)
	rstp	Rapid Spanning Tree Protocol (RSTP)
	mstp	Multiple Spanning Tree Protocol (MSTP)
	imi	Integrated Management Interface (IMI)
	imish	Integrated Management Interface Shell (IMISH)
	epsr	Ethernet Protection Switched Rings (EPSR)
	irdp	ICMP Router Discovery Protocol (IRDP)
	rmon	Remote Monitoring
	loopprot	Loop Protection
	poe	Power-inline (Power over Ethernet)
	dhcpsn	DHCP snooping (DHCPSN)
facility	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon

Parameter	Description
`msgtext`	Exclude messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log console exclude msgtext example of
irrelevant message
```

Related commands

default log console

log console

log console (filter)

show log config

log 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
<email-address>	The email address to send log messages to

Default By default no filters are defined for email log targets. Filters must be defined before messages will be sent.

Mode Global Configuration

Example To have log messages emailed to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com
```

Related commands

default log email

log email (filter)

log email exclude

log email time

show log config

log email (filter)

Overview This command creates a filter to select messages to be sent to an email address. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a specified email address. All configuration relating to this log target will be removed.

Syntax

```
log email <email-address> [level <level>] [program
<program-name>] [facility <facility>] [msgtext <text-string>]
```

```
no log email <email-address> [level <level>] [program
<program-name>] [facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
<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.	
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)
	`bgp`	Border Gateway Protocol (BGP)

Parameter	Description	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`pim-dm`	Protocol Independent Multicast - Dense Mode (PIM-DM)
	`pim-sm`	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	`pim-smv6`	PIM-SM version 6 (PIM-SMv6)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`irdp`	ICMP Router Discovery Protocol (IRDP)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Filter messages by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Select messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Mode Global Configuration

Examples To create a filter to send all messages containing the text “Bridging initialization”, to the email address admin@homebase.com, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@homebase.com msgtext "Bridging initialization"
```

To create a filter to send messages with a severity level of **informational** and above to the email address admin@alliedtelesis.com, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com level informational
```

To stop the device emailing log messages emailed to the email address admin@alliedtelesis.com, use the following commands:

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

To remove a filter that sends messages with a severity level of **informational** and above to the email address admin@alliedtelesis.com, use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@alliedtelesis.com level informational
```

Related commands

default log email

log email

log email exclude

log email time

show log config

log email exclude

Overview Use this command to prevent specified log messages from being emailed, when the device is configured to send log messages to an email address. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log email exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log email exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)

Parameter	Description	
	bgp	Border Gateway Protocol (BGP)
	rsvp	Resource Reservation Protocol (RSVP)
	pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
	pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	pim-smv6	PIM-SM version 6 (PIM-SMv6)
	dot1x	IEEE 802.1X Port-Based Access Control
	lacp	Link Aggregation Control Protocol (LACP)
	stp	Spanning Tree Protocol (STP)
	rstp	Rapid Spanning Tree Protocol (RSTP)
	mstp	Multiple Spanning Tree Protocol (MSTP)
	imi	Integrated Management Interface (IMI)
	imish	Integrated Management Interface Shell (IMISH)
	epsr	Ethernet Protection Switched Rings (EPSR)
	irdp	ICMP Router Discovery Protocol (IRDP)
	rmon	Remote Monitoring
	loopprot	Loop Protection
	poe	Power-inline (Power over Ethernet)
	dhcpsn	DHCP snooping (DHCPSN)
facility	Exclude messages from a syslog facility.	
<*facility*>	Specify one of the following syslog facilities to exclude messages from:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon

Parameter	Description
`msgtext`	Exclude messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log email exclude msgtext example of irrelevant message
```

Related commands

default log email

log email

log email (filter)

log email time

show log config

log email time

Overview This command configures the time used in messages sent to an email address. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

Syntax

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

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

Default The default is **local** time.

Mode Global Configuration

Usage notes Use the **local** option if the email recipient is in the same time zone as this device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the email recipient in hours. Messages will display the time they were generated on this device but converted to the time zone of the email recipient.

Examples

To send messages to the email address `test@home.com` in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local 0
```

To send messages to the email address `admin@base.com` with the time information converted to the time zone of the email recipient, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local-offset plus
3
```

To send messages to the email address `user@remote.com` with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email user@remote.com time utc-offset minus
3
```

Related commands

default log email

log email

log email (filter)

log email exclude

show log config

log facility

Overview Use this command to assign a facility to all log messages generated on this device. This facility overrides any facility that is automatically generated as part of the log message.

Use the **no** variant of this command to remove the configured facility.

Syntax

```
log facility {kern|user|mail|daemon|auth|syslog|lpr|news|uucp|
cron|authpriv|ftp|local0|local1|local2|local3|local4|local5|
local6|local7}
```

```
no log facility
```

Default None. The outgoing syslog facility depends on the log message.

Mode Global Configuration

Usage notes Specifying different facilities for log messages generated on different devices can allow messages from multiple devices sent to a common server to be distinguished from each other.

Ordinarily, the facility values generated in log messages have meanings as shown in the following table. Using this command will override these meanings, and the new meanings will depend on the use you put them to.

Table 7-1: Ordinary meanings of the facility parameter in log messages

Facility	Description
kern	Kernel messages
user	User-level messages
mail	Mail system
daemon	System daemons
auth	Security/authorization messages
syslog	Messages generated internally by the syslog daemon
lpr	Line printer subsystem
news	Network news subsystem
uucp	UNIX-to-UNIX Copy Program subsystem
cron	Clock daemon
authpriv	Security/authorization (private) messages

Table 7-1: Ordinary meanings of the facility parameter in log messages (cont.)

Facility	Description
ftp	FTP daemon
local<0..7>	The facility labels above have specific meanings, while the local facility labels are intended to be put to local use. In AlliedWare Plus, some of these local facility labels are used in log messages. In particular, local5 is assigned to log messages generated by UTM Firewall security features.

Example To specify a facility of local6, use the following commands:

```
awplus# configure terminal
awplus(config)# log facility local6
```

Related commands show log config

log host

Overview This command configures the device to send log messages to a remote syslog server via UDP port 514. The IP address of the remote server must be specified. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent.

Use the **no** variant of this command to stop sending log messages to the remote syslog server.

Syntax

```
log host <ipv4-addr> [secure]
log host <ipv6-addr>
no log host <ipv4-addr>|<ipv6-addr>
```

Parameter	Description
<ipv4-addr>	Specify the source IPv4 address, in dotted decimal notation (A.B.C.D).
<ipv6-addr>	Specify the source IPv6 address, in X:X::X:X notation.
secure	Optional value to create a secure log destination. This option is only valid for IPv4 hosts.

Mode Global Configuration

Usage notes Use the optional **secure** parameter to configure a secure IPv4 syslog host. For secure hosts, syslog over TLS is used to encrypt the logs. The certificate received from the remote log server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

The remote server may also request that a certificate is transmitted from the local device. In this situation the first trustpoint added to the syslog application will be transmitted to the remote server.

For detailed information about securing syslog, see the PKI Feature Overview_and Configuration_Guide.

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

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

To stop the device from sending log messages to the remote syslog server with IP address 10.32.16.99, use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.99
```

Related commands default log host

log host (filter)

log host exclude

log host source

log host startup-delay

log host time

log trustpoint

show log config

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log host (filter)

Overview This command creates a filter to select messages to be sent to a remote syslog server. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a substring within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a remote syslog server. The IP address of the syslog server must be specified. All configuration relating to this log target will be removed.

Syntax

```
log host <ip-addr> [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]

no log host <ip-addr> [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
<ip-addr>	The IP address of a remote syslog server.	
`level`	Filter messages by severity level.	
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages by program. Include messages from a specified program.	
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)
	`bgp`	Border Gateway Protocol (BGP)
	`rsvp`	Resource Reservation Protocol (RSVP)

Parameter	Description	
	`pim-dm`	Protocol Independent Multicast - Dense Mode (PIM-DM)
	`pim-sm`	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	`pim-smv6`	PIM-SM version 6 (PIM-SMv6)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`irdp`	ICMP Router Discovery Protocol (IRDP)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Filter messages by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Select messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Mode Global Configuration

Examples To create a filter to send all messages containing the text “Bridging initialization”, to a remote syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 msgtext "Bridging
initialization"
```

To create a filter to send messages with a severity level of **informational** and above to the syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 level informational
```

To remove a filter that sends all messages containing the text “Bridging initialization”, to a remote syslog server with IP address 10.32.16.21, use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.21 msgtext "Bridging
initialization"
```

To remove a filter that sends messages with a severity level of **informational** and above to the syslog server with IP address 10.32.16.21, use the following commands:

```
awplusawpluls# configure terminal
awplus(config)# no log host 10.32.16.21 level informational
```

Related commands

default log host

log host

log host exclude

log host source

log host time

show log config

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log host exclude

Overview Use this command to prevent specified log messages from being sent to the remote syslog server, when log host is enabled. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log host {<hostname>|<ipv4-addr>|<ipv6-addr>} exclude [level
<level>] [program <program-name>] [facility <facility>]
[msgtext <text-string>]
```

```
no log host {<hostname>|<ipv4-addr>|<ipv6-addr>} exclude [level
<level>] [program <program-name>] [facility <facility>]
[msgtext <text-string>]
```

Parameter	Description	
<hostname>	The host name of a remote syslog server.	
<ipv4-addr>	The IPv4 address of a remote syslog server, in A.B.C.D format.	
<ipv6-addr>	The IPv6 address of a remote syslog server, in X:X::X:X format.	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	

Parameter	Description	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)
	`bgp`	Border Gateway Protocol (BGP)
	`rsvp`	Resource Reservation Protocol (RSVP)
	`pim-dm`	Protocol Independent Multicast - Dense Mode (PIM-DM)
	`pim-sm`	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	`pim-smv6`	PIM-SM version 6 (PIM-SMv6)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`irdp`	ICMP Router Discovery Protocol (IRDP)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon

Parameter	Description	
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Exclude messages containing a certain text string.	
`<text-string>`	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default No log messages are excluded

Mode Global configuration

Example To exclude messages that contain the string 'example of irrelevant message' being sent to the remote syslog server 10.10.10.100, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.10.10.100 exclude msgtext example
of irrelevant message
```

Related commands

default log host

log host

log host (filter)

log host source

log host time

show log config

Command changes Version 5.2.2-1.1: **vrf** parameter added for products that support VRF

log host source

Overview Use this command to specify a source interface or IP address for the device to send syslog messages from. You can specify any one of an interface name, an IPv4 address or an IPv6 address.

This is useful if the device can reach the syslog server via multiple interfaces or addresses and you want to control which interface/address the device uses.

Note that AlliedWare Plus does not support source interface settings on secure log hosts (which are hosts configured using "log host <ip-address> secure").

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

Syntax

```
log host source {<interface-name>|<ipv4-addr>|<ipv6-addr>}
no log host source
```

Parameter	Description
<interface-name>	Specify the source interface name. You can enter a VLAN, eth interface or loopback interface.
<ipv4-addr>	Specify the source IPv4 address, in dotted decimal notation (A.B.C.D).
<ipv6-addr>	Specify the source IPv6 address, in X:X::X:X notation.

Default None (no source is configured)

Mode Global Configuration

Example To send syslog messages from 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# log host source 192.168.1.1
```

Related commands

default log host

log host

log host (filter)

log host exclude

log host time

show log config

log host startup-delay

Overview Use this command to set the delay between the device booting up and it attempting to connect to remote log hosts. This is to allow time for network connectivity to the remote host to be established. During this period, the device buffers log messages and sends them once it has connected to the remote host.

The startup delay begins when the message "syslog-ng starting up" appears in the log.

If the default startup delay is not long enough for the boot and configuration process to complete and the links to come up, you may see logging failure messages on startup. In these cases, you can use the command to increase the startup delay.

Use the **no** variant of this command to return to the default delay values.

Syntax

```
log host startup-delay [delay <1-600>] [messages <1-5000>]
no log host startup-delay
```

Parameter	Description
`delay <1-600>`	The time, in seconds, from when syslog starts before the device attempts to filter and transmit the buffered messages to remote hosts.
`messages <1-5000>`	The maximum number of messages that the device will buffer during the delay period.

Default By default the system will buffer up to 2000 messages and wait 120 seconds from when syslog starts before attempting to filter and transmit the buffered messages to remote hosts.

Mode Global Configuration

Example To increase the delay to 180 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# log host startup-delay delay 180
```

Related commands

default log host

log host (filter)

log host exclude

log host source

log host time

log trustpoint

show log config

Command changes Version 5.4.8-0.2: defaults changed

log host time

Overview This command configures the time used in messages sent to a remote syslog server. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

Syntax

```
log host {<hostname>|<ipv4-addr>|<ipv6-addr>} time
{local|local-offset|utc-offset {plus|minus} <0-24>}
```

Parameter	Description
<hostname>	The host name of a remote syslog server.
<ipv4-addr>	The IPv4 address of a remote syslog server, in A.B.C.D format.
<ipv6-addr>	The IPv6 address of a remote syslog server, in X:X::X:X format.
<email-address>	The email address to send log messages to
`time`	Specify the time difference between the email recipient and the device you are configuring.
`local`	The device is in the same time zone as the email recipient
`local-offset`	The device is in a different time zone to the email recipient. Use the **plus** or **minus** keywords and specify the difference (offset) from local time of the device to the email recipient in hours.
`utc-offset`	The device is in a different time zone to the email recipient. Use the **plus** or **minus** keywords and specify the difference (offset) from UTC time of the device to the email recipient in hours.
`plus`	Negative offset (difference) from the device to the syslog server.
`minus`	Positive offset (difference) from the device to the syslog server.
<0-24>	World Time zone offset in hours

Default The default is **local** time.

Mode Global Configuration

Usage notes Use the **local** option if the remote syslog server is in the same time zone as the device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the remote syslog server in hours. Messages will display the time they were generated on this device but converted to the time zone of the remote syslog server.

Examples

To send messages to the remote syslog server with the IP address 10.32.16.21 in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 time local 0
```

To send messages to the remote syslog server with the IP address 10.32.16.12 with the time information converted to the time zone of the remote syslog server, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.12 time local-offset plus 3
```

To send messages to the remote syslog server with the IP address 10.32.16.02 with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.02 time utc-offset minus 3
```

Related commands

default log host

log host

log host (filter)

log host exclude

log host source

show log config

Command changes

Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

log monitor (filter)

Overview This command creates a filter to select messages to be sent to the terminal when the terminal monitor command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

Syntax

```
log monitor [level <level>] [program <program-name>] [facility
<facility>] [msgtext <text-string>]

no log monitor [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Filter messages by severity level.	
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages by program. Include messages from a specified program.	
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)
	`bgp`	Border Gateway Protocol (BGP)
	`rsvp`	Resource Reservation Protocol (RSVP)
	`pim-dm`	Protocol Independent Multicast - Dense Mode (PIM-DM)
	`pim-sm`	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	`pim-smv6`	PIM-SM version 6 (PIM-SMv6)

Parameter	Description	
	dot1x	IEEE 802.1X Port-Based Access Control
	lacp	Link Aggregation Control Protocol (LACP)
	stp	Spanning Tree Protocol (STP)
	rstp	Rapid Spanning Tree Protocol (RSTP)
	mstp	Multiple Spanning Tree Protocol (MSTP)
	imi	Integrated Management Interface (IMI)
	imish	Integrated Management Interface Shell (IMISH)
	epsr	Ethernet Protection Switched Rings (EPSR)
	irdp	ICMP Router Discovery Protocol (IRDP)
	rmon	Remote Monitoring
	loopprot	Loop Protection
	poe	Power-inline (Power over Ethernet)
	dhcpsn	DHCP snooping (DHCPSN)
facility	Filter messages by syslog facility.	
<*facility*>	Specify one of the following syslog facilities to include messages from:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon
msgtext	Select messages containing a certain text string.	
<*text-string*>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default By default there is a filter to select all messages. This filter may be removed and replaced by filters that are more selective.

Mode Global Configuration

Examples

To create a filter to send all messages that are generated by authentication and have a severity of **info** or higher to terminal instances where the terminal monitor command has been given, use the following commands:

```
awplus# configure terminal
awplus(config)# log monitor level info program auth
```

To remove a default filter that includes sending everything to the terminal, use the following commands:

```
awplus# configure terminal
awplus(config)# no log monitor level debugging
```

Related commands

default log monitor

log monitor exclude

show log config

terminal monitor

log monitor exclude

Overview Use this command to prevent specified log messages from being displayed on a terminal, when terminal monitor is enabled. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)

Parameter	Description	
	bgp	Border Gateway Protocol (BGP)
	rsvp	Resource Reservation Protocol (RSVP)
	pim-dm	Protocol Independent Multicast - Dense Mode (PIM-DM)
	pim-sm	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	pim-smv6	PIM-SM version 6 (PIM-SMv6)
	dot1x	IEEE 802.1X Port-Based Access Control
	lacp	Link Aggregation Control Protocol (LACP)
	stp	Spanning Tree Protocol (STP)
	rstp	Rapid Spanning Tree Protocol (RSTP)
	mstp	Multiple Spanning Tree Protocol (MSTP)
	imi	Integrated Management Interface (IMI)
	imish	Integrated Management Interface Shell (IMISH)
	epsr	Ethernet Protection Switched Rings (EPSR)
	irdp	ICMP Router Discovery Protocol (IRDP)
	rmon	Remote Monitoring
	loopprot	Loop Protection
	poe	Power-inline (Power over Ethernet)
	dhcpsn	DHCP snooping (DHCPSN)
facility	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon

Parameter	Description
`msgtext`	Exclude messages containing a certain text string.
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log monitor exclude msgtext example of
irrelevant message
```

Related commands

default log monitor

log monitor (filter)

show log config

terminal monitor

log permanent

Overview This command configures the device to send permanent log messages to non-volatile storage (NVS) on the device. The content of the permanent log is retained over a reboot. Once the permanent log reaches its configured maximum allowable size old messages will be deleted to make way for new messages.

The **no** variant of this command configures the device not to send any messages to the permanent log. Log messages will not be retained over a restart.

Syntax

```
log permanent
no log permanent
```

Mode Global Configuration

Examples To enable permanent logging use the following commands:

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

To disable permanent logging use the following commands:

```
awplus# configure terminal
awplus(config)# no log permanent
```

Related commands

clear log permanent

copy permanent-log

default log permanent

log permanent (filter)

log permanent exclude

log permanent size

show log config

show log permanent

log permanent (filter)

Overview This command creates a filter to select messages to be sent to the permanent log. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the permanent log.

Syntax

```
log permanent [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log permanent [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Filter messages sent to the permanent log by severity level.	
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages by program. Include messages from a specified program.	
<program-name>	The name of a program to log messages from. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)
	`bgp`	Border Gateway Protocol (BGP)
	`rsvp`	Resource Reservation Protocol (RSVP)
	`pim-dm`	Protocol Independent Multicast - Dense Mode (PIM-DM)
	`pim-sm`	Protocol Independent Multicast - Sparse Mode (PIM-SM)

Parameter	Description	
	`pim-smv6`	PIM-SM version 6 (PIM-SMv6)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`irdp`	ICMP Router Discovery Protocol (IRDP)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Filter messages by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Select messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default By default the buffered log has a filter to select messages whose severity level is `notices (5)` or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To create a filter to send all messages containing the text "`Bridging initialization`", to the permanent log use the following commands:

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

Related commands

clear log permanent

default log permanent

log permanent

log permanent exclude

log permanent size

show log config

show log permanent

log permanent exclude

Overview Use this command to prevent specified log messages from being sent to the permanent log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log permanent exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log permanent exclude [level <level>] [program
<program-name>] [facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. You can enter either one of the following predefined program names (depending on your device model), or another program name that you find in the log output. The pre-defined names are not case sensitive but other program names from the log output are.	
	`rip`	Routing Information Protocol (RIP)
	`ripng`	Routing Information Protocol - next generation (RIPng)
	`ospf`	Open Shortest Path First (OSPF)
	`ospfv3`	Open Shortest Path First (OSPF) version 3 (OSPFv3)
	`bgp`	Border Gateway Protocol (BGP)

Parameter	Description	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`pim-dm`	Protocol Independent Multicast - Dense Mode (PIM-DM)
	`pim-sm`	Protocol Independent Multicast - Sparse Mode (PIM-SM)
	`pim-smv6`	PIM-SM version 6 (PIM-SMv6)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`irdp`	ICMP Router Discovery Protocol (IRDP)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Exclude messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent exclude msgtext example of
irrelevant message
```

Related commands

clear log permanent

default log permanent

log permanent

log permanent (filter)

log permanent size

show log config

show log permanent

log permanent size

Overview This command configures the amount of memory that the permanent log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

Use the **no** variant of this command to return to the default.

Syntax

```
log permanent size <50-250>
no log permanent size
```

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

Default 50 kilobytes

Mode Global Configuration

Example To allow the permanent log to use up to 100 kilobytes of NVS, use the commands:

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

To return to the default value, use the commands:

```
awplus# configure terminal
awplus(config)# no log permanent size
```

Related commands

clear log permanent

copy permanent-log

default log permanent

log permanent

log permanent (filter)

log permanent exclude

show log config

show log permanent

log-rate-limit nsm

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

Use the **no** variant of this command to revert to the default number of log messages, which is up to 200 log messages per second.

Syntax

```
log-rate-limit nsm messages <message-limit> interval
<time-interval>
```

```
no log-rate-limit nsm
```

Parameter	Description
<message-limit>	<1-65535> The number of log messages generated by the device.
<time-interval>	<0-65535> The time period for log message generation in 1/100 seconds. If an interval of 0 is specified then no log message rate limiting is applied.

Default By default, the device will allow 200 log messages to be generated per second.

Mode Global Configuration

Usage notes This command limits the rate that log messages are generated. Limiting log messages protects the device from running out of memory in extreme conditions, such as during a broadcast storm.

Once the specified number of log messages per interval is exceeded, any excess log messages are dropped. When this occurs a summary log message is generated at the end of the interval. This summary message includes the number of log messages dropped.

If you expect a lot of dropped log messages, we recommend setting the time interval to no less than 100. This limits the number of summary messages to one per second, which prevents the log from filling up with these summary messages.

Examples To allow the device to generate a maximum of 300 log messages per second, use the following commands:

```
awplus# configure terminal
awplus(config)# log-rate-limit nsm messages 300 interval 100
```

To return the device to the default setting, use the following commands:

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

log trustpoint

Overview This command adds one or more trustpoints to be used with the syslog application. Multiple trustpoints may be specified, or the command may be executed multiple times, to add multiple trustpoints to the application.

The **no** version of this command removes one or more trustpoints from the list of trustpoints associated with the application.

Syntax

```
log trustpoint [<trustpoint-list>]
no log trustpoint [<trustpoint-list>]
```

Parameter	Description
<trustpoint-list>	Specify one or more trustpoints to be added or deleted.

Default No trustpoints are created by default.

Mode Global Configuration

Usage notes The device certificate associated with first trustpoint added to the application will be transmitted to remote servers. The certificate received from the remote server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

If no trustpoints are specified in the command, the trustpoint list will be unchanged.

If **no log trustpoint** is issued without specifying any trustpoints, then all trustpoints will be disassociated from the application.

Example You can add multiple trustpoints by executing the command multiple times:

```
awplus# configure terminal
awplus(config)# log trustpoint trustpoint_1
awplus(config)# log trustpoint trustpoint_2
```

Alternatively, add multiple trustpoints with a single command:

```
awplus(config)# log trustpoint trustpoint_2 trustpoint_3
```

Disassociate all trustpoints from the syslog application using the command:

```
awplus(config)# log trustpoint trustpoint_2 trustpoint_3
```

Related commands log host

show log config

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 7-1: 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 8: Parameters in output of the **show counter log** command

Parameter	Description
Total Received	Total number of messages received by the log
Total Received P0	Total number of Priority 0 (Emergency) messages received
Total Received P1	Total number of Priority 1 (Alert) messages received
Total Received P2	Total number of Priority 2 (Critical) messages received
Total Received P3	Total number of Priority 3 (Error) messages received
Total Received P4	Total number of Priority 4 (Warning) messages received
Total Received P5	Total number of Priority 5 (Notice) messages received
Total Received P6	Total number of Priority 6 (Info) messages received
Total Received P7	Total number of Priority 7 (Debug) messages received

Related commands show log config

show exception log

Overview This command displays the contents of the exception log. If the device has unexpectedly restarted and has produced a core dump file, the output of this command shows the name and location of the file.

Syntax

```
show exception log
```

Mode User Exec and Privileged Exec

Example To display the exception log, use the command:

```
awplus# show exception log
```

Output Figure 7-2: Example output from the **show exception log** command on a device that has never had an exception occur

```
awplus#show exception log
<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
None
------------------------------------------------------------------------
awplus#
```

show log

Overview This command displays the contents of the buffered log.

For information on filtering and saving command output, see the "Getting Started with AlliedWare_Plus" Feature Overview and Configuration Guide.

Syntax

```
show log [tail [<10-250>]]
```

Parameter	Description
`tail`	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Default By default the entire contents of the buffered log is displayed.

Mode User Exec, Privileged Exec and Global Configuration

Usage notes If the optional **tail** parameter is specified, only the latest 10 messages in the buffered log are displayed. A numerical value can be specified after the **tail** parameter to select how many of the latest messages should be displayed.

The **show log** command is only available to users at privilege level 7 and above. To set a user's privilege level, use the command:

```
awplus(config)# username <name> privilege <1-15>
```

Examples To display the contents of the buffered log use the command:

```
awplus# show log
```

To display the 10 latest entries in the buffered log use the command:

```
awplus# show log tail 10
```

Output Figure 7-3: Example output from **show log**

```
awplus#show log

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2023 May 29 07:55:22 kern.warning awplus kernel: No pci config register base in
dev tree, using default
2023 May 29 07:55:23 kern.notice awplus kernel: Kernel command line: console=tty
S0,9600 releasefile= ramdisk=14688 bootversion=1.1.0 loglevel=1 extraflash=00000000
2023 May 29 07:55:25 kern.notice awplus kernel: RAMDISK: squashfs filesystem fou
nd at block 0
2023 May 29 07:55:28 kern.warning awplus kernel: ipifwd: module license 'Proprie
tary' taints kernel.
...
```

Related commands

clear log buffered

copy buffered-log

default log buffered

log buffered

log buffered (filter)

log buffered size

log buffered exclude

show log config

show log config

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

Syntax

```
show log config
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the logging configuration use the command:

```
awplus# show log config
```

Output Figure 7-4: Example output from **show log config**

```
Facility: default

PKI trustpoints: example_trustpoint

Buffered log:
 Status ......... enabled
  Maximum size ... 100kb
  Filters:
 *1 Level ........ notices
    Program ...... any
    Facility ..... any
    Message text . any
  2 Level ........ informational
    Program ...... auth
    Facility ..... daemon
    Message text . any
  Statistics ..... 1327 messages received, 821 accepted by filter (2016 Oct 11
10:36:16)
Permanent log:
  Status ......... enabled
  Maximum size ... 60kb
  Filters:
  1 Level ........ error
    Program ...... any
    Facility ..... any
    Message text . any
 *2 Level ........ warnings
    Program ...... dhcp
    Facility ..... any
    Message text . "pool exhausted"
  Statistics ..... 1327 messages received, 12 accepted by filter (2016 Oct 11
10:36:16)
```

```
Host 10.32.16.21:
  Time offset .... +2:00
  Offset type .... UTC
  Source ......... -
  Secured ........ enabled
  Filters:
  1 Level ........ critical
    Program ...... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 1 accepted by filter (2016 Oct 11
10:36:16)
Email admin@alliedtelesis.com:
  Time offset .... +0:00
  Offset type .... Local
  Filters:
  1 Level ........ emergencies
    Program ...... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 0 accepted by filter (2016 Oct 11
10:36:16)
...
```

In the above example the '*' next to filter 1 in the buffered log configuration indicates that this is the default filter. The permanent log has had its default filter removed, so none of the filters are marked with '*'.

NOTE: *Terminal log and console log cannot be set at the same time. If console logging is enabled then the terminal logging is turned off.*

Related commands

show counter log

show log

show log permanent

show log permanent

Overview This command displays the contents of the permanent log.

Syntax

```
show log permanent [tail [<10-250>]]
```

Parameter	Description
`tail`	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Usage notes If the optional **tail** parameter is specified, only the latest 10 messages in the permanent log are displayed. A numerical value can be specified after the **tail** parameter to change how many of the latest messages should be displayed.

Mode User Exec, Privileged Exec and Global Configuration

Example To display the permanent log, use the command:

```
awplus# show log permanent
```

Output Figure 7-5: Example output from **show log permanent**

```
awplus> show log permanent

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2025 Apr 22 14:14:32 user.err VAA-Controller IMISH[93540]: Command [sconf t] failed
2025 Apr 22 14:16:29 user.err VAA-Controller IMISH[93540]: Command [eth0] failed
2025 Apr 22 14:18:37 local6.crit VAA-Controller ATMF[960]: x610-link-sw has left. 1
member in total.
2025 Apr 22 14:18:39 local6.crit VAA-Controller ATMF[960]: x610-link-sw has joined.
2 members in total.
2025 Apr 22 14:30:12 user.err VAA-Controller IMISH[93540]: Command [del del
vaa-5.4.9-2.1.iso] failed
2025 Apr 22 14:57:23 user.err VAA-Controller IMISH[93540]: Command [service http]
failed
2025 Apr 22 15:01:45 user.err VAA-Controller IMISH[93540]: Command [update webgui
now] failed
...
```

Related commands

clear log permanent

copy permanent-log

default log permanent

log permanent

log permanent (filter)

log permanent exclude

log permanent size

show log config

show running-config log

Overview This command displays the current running configuration of the Log utility.

Syntax

```
show running-config log
```

Mode Privileged Exec and Global Configuration

Example To display the current configuration of the log utility, use the command:

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

Related commands show log

show log config

8 Scripting Commands

Introduction

Overview This chapter provides commands used for command scripts.

Command List

- "activate" on page 285
- "echo" on page 286
- "wait" on page 287

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 **.scp** or a **.sh** filename extension for a valid script text file, as described below in the usage section for this command.

Mode Privileged Exec

Usage notes When a script is activated, the privilege level is set to 1 enabling User Exec commands to run in the script. If you need to run Privileged Exec commands in your script you need to add an enable (Privileged Exec mode) command to the start of your script. If you need to run Global Configuration commands in your script you need to add a configure terminal command after the **enable** command at the start of your script.

The **activate** command executes the script in a new shell. A terminal length shell command, such as **terminal length 0** may also be required to disable a delay that would pause the display.

A script must be a text file with a filename extension of either **.sh** or **.scp** only for the AlliedWare Plus CLI to activate the script file. The **.sh** filename extension indicates the file is an ASH script, and the **.scp** filename extension indicates the file is an AlliedWare Plus script.

Examples To activate a command script to run as a background process, use the command:

```
awplus#activate background test.scp
```

Related commands

configure terminal

echo

enable (Privileged Exec mode)

wait

echo

Overview This command echoes a string to the terminal, followed by a blank line.

Syntax

```
echo <line>
```

Parameter	Description
<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>	<1-65535> Specify the time delay in seconds

Default No wait delay is specified by default.

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

Usage notes Use this command to pause script execution in an **.scp** (AlliedWare Plus™ script) or an **.sh** (ASH script) file executed by the activate command. The script must contain an **enable** command, because the **wait** command is only executed in the Privileged Exec mode.

Example See an **.scp** script file extract below that will show port counters for interface eth0 over a 10 second interval:

```
enable

show interface eth0

wait 10

show interface eth0
```

Related commands

activate

echo

enable (Privileged Exec mode)

9 Interface Commands

Introduction

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

Command List

- "description (interface)" on page 289
- "interface (to configure)" on page 290
- "mtu" on page 292
- "service statistics interfaces counter" on page 294
- "show interface" on page 295
- "show interface brief" on page 298
- "show interface memory" on page 299
- "show interface status" on page 301
- "shutdown" on page 303

description (interface)

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

Syntax

```
description <description>
```

Parameter	Description
<description>	Text describing the specific interface. Descriptions can contain any printable ASCII characters (ASCII 32-126).

Mode Interface Configuration

Example The following example uses this command to describe the device that an interface is connected to.

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# description Master Link
```

Command changes Version 5.4.7-1.1: valid character set changed to printable ASCII characters

interface (to configure)

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

Syntax

```
interface <interface-list>
```

Parameter	Description
<interface-list>	The interfaces to configure. An interface-list can be: • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the **encapsulation dot1q** command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. The specified interfaces must exist.

Usage notes A local loopback interface is one that is always available for higher layer protocols to use and advertise to the network. Although a local loopback interface is assigned an IP address, it does not have the usual requirement of connecting to a lower layer physical entity. This lack of physical attachment creates the perception of a local loopback interface always being accessible via the network.

Local loopback interfaces can be utilized by a number of protocols for various purposes. They can be used to improve access to the device and also increase its reliability, security, scalability and protection. In addition, local loopback interfaces can add flexibility and simplify management, information gathering and filtering.

Mode Global Configuration

Examples The following example shows how to enter Interface mode to configure the Ethernet interface eth0.2. Note how the prompt changes.

```
awplus# configure terminal
awplus(config)# interface eth0.2
awplus(config-if)#
```

The following example shows how to enter Interface mode to configure the local loopback interface.

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)#
```

Related commands

ip address (IP Addressing and Protocol)

show interface

show interface brief

mtu

Overview Use this command to set the Maximum Transmission Unit (MTU) size for interfaces, where MTU is the maximum packet size that interfaces can transmit. The MTU size setting is applied to both IPv4 and IPv6 packet transmission.

Use the **no** variant of this command to remove a previously specified Maximum Transmission Unit (MTU) size, and restore the default MTU size. For example, the VLAN interface default is 1500 bytes.

Syntax

```
mtu <68-1582>
no mtu
```

Parameter	Description
<68-1582>	The Maximum Transmission size in bytes.

Default The default MTU size, for example 1500 bytes for VLAN interfaces.

Mode Interface Configuration

Usage notes If a device receives an IPv4 packet for Layer 3 switching to another interface with an MTU size smaller than the packet size, and if the packet has the '**don't fragment**' bit set, then the device will send an ICMP '**destination unreachable**' (3) packet type and a '**fragmentation needed and DF set**' (4) code back to the source. For IPv6 packets bigger than the MTU size of the transmitting interface, an ICMP '**packet too big**' (ICMP type 2 code 0) message is sent to the source.

You can set a feasible MTU value on the following interfaces:

- Ethernet
- Tunnel

Note that you cannot configure MTU on bridge interfaces. The MTU of the bridge interface is determined by the member interface of the bridge which has the lowest MTU. For example, if you attach eth0 with MTU 1200 and tunnel1 with MTU 1500 to a bridge interface, the MTU for that interface will be 1200.

Examples To configure an MTU size of 1555 bytes for tunnel 'tunnel2', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# mtu 1555
```

Related commands show interface

Command changes Version 5.4.7-1.1: Behavior change when MTU set to less than 1500 on FS980M and GS980M.

Version 5.5.1-0.1: Layer 3 jumbo frames supported on SBx908 GEN2 and x950.

Version 5.5.1-1.2: Layer 3 jumbo frames supported on x530 and GS980MX.

service statistics interfaces counter

Overview Use this command to enable the interface statistics counter.

Use the **no** variant of this command to disable the interface statistics counter.

Syntax

```
service statistics interfaces counter
no service statistics interfaces counter
```

Default The interface statistics counter is enabled by default.

Mode Global Configuration

Example To enable the interface statistics counter, use the following commands:

```
awplus# configure terminal
awplus(config)# service statistics interfaces counter
```

To disable the interface statistics counter, use the following commands:

```
awplus# configure terminal
awplus(config)# no service statistics interfaces counter
```

Command changes Version 5.4.7-2.1: command added

show interface

Overview Use this command to display interface configuration and status.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show interface [<interface-list>]
```

Parameter	Description
<interface-list>	The interfaces or ports to display. An interface-list can be: • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the **encapsulation dot1q** command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. The specified interfaces must exist.

Mode User Exec and Privileged Exec

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

```
awplus# show interface
```

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

```
awplus# show interface lo
```

To display configuration and status information for eth0.2, use the command:

```
awplus# show interface eth0.2
```

Output Figure 9-1: Example output from the **show interface** command:

```
awplus#show interface
Interface eth0
  Link is UP, administrative state is UP
  Hardware is Ethernet, address is ce7f.dc5d.b53e
  index 3 metric 1 mtu 1500
  current duplex full, current speed 1000, current polarity mdi
  configured duplex auto, configured speed auto, configured polarity auto
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 39994480, bytes 4659884105, dropped 0, multicast packets 0
    output packets 31645676, bytes 5366141711
    input average rate : 30 seconds 120.83 Kbps, 5 minutes 80.63 Kbps
    output average rate: 30 seconds 108.47 Kbps, 5 minutes 84.53 Kbps
    input peak rate 44.41 Mbps at 2020/06/19 03:00:07
    output peak rate 4.41 Mbps at 2020/06/25 01:05:51
  Time since last state change: 6 days 20:51:11
...
```

Figure 9-2: 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
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
  Time since last state change: 8 days 00:01:09
```

Figure 9-3: Example output from the **show interface eth0.2** command:

```
awplus#show interface eth0.2
  Link is UP, administrative state is UP
  Hardware is Encapsulated Ethernet, address is ce7f.dc5d.b53e
  IPv4 address 192.168.2.1/24 broadcast 192.168.2.255
  Description: area2
  index 10 metric 1 mtu 1500
  802.1Q VID 2 over eth0
  <UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 2177306, bytes 1285365908, dropped 0, multicast packets 0
    output packets 1317871, bytes 223426881
    input average rate : 30 seconds 2.65 Kbps, 5 minutes 14.52 Kbps
    output average rate: 30 seconds 1.03 Kbps, 5 minutes 2.79 Kbps
    input peak rate 44.23 Mbps at 2020/06/19 03:00:07
    output peak rate 2.12 Mbps at 2020/06/19 03:00:07
  Time since last state change: 6 days 21:21:469
```

Related commands

mtu

show interface brief

show interface status

Command changes

Version 5.4.7-2.1: average rate and peak rate added to output

show interface brief

Overview Use this command to display brief interface, configuration, and status information, including provisioning information.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show interface brief
```

Mode User Exec and Privileged Exec

Example To display summarized information about all interfaces on the device, use the command:

```
awplus# show interface brief
```

Output Figure 9-4: Example output from **show interface brief**

```
awplus#show interface brief
Interface              Status          Protocol
eth0                   admin up        running
eth0.3                 admin up        running
eth0.2                 admin up        running
lo                     admin up        running
br0                    admin up        down
```

Table 9-1: Parameters in the output of **show interface brief**

Parameter	Description
`Interface`	The name or type of interface.
`Status`	The administrative state. This can be either **admin up** or **admin down**.
`Protocol`	The link state. This can be either **down**, **running**, or **provisioned**.

Related commands

show interface

show interface status

show interface memory

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 the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show interface memory
show interface <port-list> memory
```

Parameter	Description
<port-list>	Display information about only the specified port or ports. The port list can be: • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the **encapsulation dot1q** command). Ranges of sub-interfaces are not supported. • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list.

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 eth0, use the command:

```
awplus# show interface eth0 memory
```

Output Figure 9-5: Example output from the **show interface memory** command

```
awplus#show interface memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
eth0         393228       512            1
lo           425997       512            1
br1          557073       512            1
```

Figure 9-6: Example output from **show interface <port-list> memory** for a list of interfaces

```
awplus#show interface eth0 memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
eth0         393228       512            1
```

Related commands

show interface brief

show interface status

show interface status

Overview Use this command to display the status of the specified interface or interfaces. Note that when no interface or interfaces are specified then the status of all interfaces on the device are shown.

Syntax

```
show interface [<port-list>] status
```

Parameter	Description
<port-list>	The ports to display information about. The port list can be: • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the **encapsulation dot1q** command). Ranges of sub-interfaces are not supported. • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list.

Examples To display the status of eth0.2 and eth0.3, use the command:

```
awplus# show interface eth0.2,eth0.3 status
```

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

```
awplus# show interface status
```

Output

Table 10: Example output from the **show interface <port-list> status** command

```
awplus#show interface eth0.2,eth0.3 status
Port       Name               Status            Vlan Duplex   Speed Type
eth0.2     area2              connected         none a-full  a-1000
eth0.3     area3              connected         none a-full  a-1000
```

Table 11: Example output from the **show interface status** command

```
awplus#show interface status
Port      Name               Status            Vlan Duplex   Speed Type
eth0                         connected         none a-full  a-1000 1000BASE-T
eth0.3    area3              connected         none a-full  a-1000
eth0.2    area2              connected         none a-full  a-1000
...
```

Table 12: Parameters in the output from the **show interface status** command

Parameter	Description
`Port`	Name/Type of the interface.
`Name`	Description of the interface.
`Status`	The administrative and operational status of the interface; one of: • disabled: the interface is administratively down. • connect: the interface is operationally up. • notconnect: the interface is operationally down.
`Vlan`	VLAN type or VLAN IDs associated with the port: • When the port is an Eth port, it displays **none**: there is no VLAN associated with it.
`Duplex`	The actual duplex mode of the interface, preceded by **a-** if it has autonegotiated this duplex mode. If the port is disabled or not connected, it displays the configured duplex setting.
`Speed`	The actual link speed of the interface, preceded by **a-** if it has autonegotiated this speed. If the port is disabled or not connected, it displays the configured speed setting.
`Type`	The type of interface, e.g. 1000BaseTX.

Related commands

show interface

show interface brief

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 bring the link back up again.

Syntax

```
shutdown
no shutdown
```

Mode Interface Configuration

Example To shut down eth0, use the commands:

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

To bring up eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no shutdown
```

Part 2: Interfaces and Layer 2

10 Bridging Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure bridging. For more information, see the Bridging Feature Overview and Configuration Guide.

Command List

- "ageing-time" on page 306
- "bridge" on page 307
- "bridge-group" on page 308
- "l3-filtering enable" on page 310
- "mac-learning" on page 311
- "show bridge" on page 312
- "show bridge macaddr" on page 314

ageing-time

Overview This command specifies the time period that a learned MAC address will remain defined within the bridge's MAC address table.

Use the **no** variant of this command to set the ageing out time back to the default.

Syntax

```
ageing-time <10-1000000>
no ageing-time
```

Parameter	Description
<10-1000000>	The number of seconds that the MAC addresses will remain in the table.

Default 300 seconds (5 minutes)

Mode Interface Configuration

Examples To change the ageing time on br2 to 60 seconds (1 minute), use the following commands:

```
awplus#configure terminal
awplus(config)#interface br2
awplus(config-if)#ageing-time 60
```

To reset the ageing time back to its default, use the following commands:

```
awplus#configure terminal
awplus(config-if)#no ageing-time
```

To reset the ageing time back to its default, you can also use the following commands:

```
awplus#configure terminal
awplus(config-if)#ageing-time 300
```

Output None

Related commands bridge

bridge-group

show bridge

show bridge macaddr

bridge

Overview Use this command to create a software bridge.

Use the **no** variant of this command to remove the specified bridge.

Syntax

```
bridge <bridge-id>
no bridge <bridge-id>
```

Parameter	Description
<bridge-id>	The bridge ID (from 1 to 300).

Default No configured bridges

Mode Global Configuration

Usage notes The bridge interface name will be prefixed with 'br' followed by the bridge ID.

If interfaces exist on a bridge, then the bridge cannot be removed. For example if interface eth1 exists on bridge 2, then the ***no bridge 2*** *command will give you the following message:*

```
% failed to remove interface br2, there are still configured
sub-interfaces.
```

Example To create a bridge with the ID of 2, use the following commands:

```
awplus#configure terminal
awplus(config)#bridge 2
```

To remove the bridge with the ID of 2, use the following commands:

```
awplus#configure terminal
awplus(config)##no bridge 2
```

Related commands

ageing-time

bridge-group

show bridge

show bridge macaddr

Command changes Version 5.5.4-0.1: maximum valid ID number changed to 300

bridge-group

Overview Use this command to add an interface to a bridge. Interfaces that have been added to a bridge will lose their L3 properties.

Use the **no** variant of this command to remove an interface from a bridge.

Syntax

```
bridge-group <0-255> [port-protected]
no bridge-group
```

Parameter	Description
<0-255>	The ID of the bridge that you are adding the interface to. Interface ID 0 is a VLAN-aware bridge.

Default Interfaces do not belong to any bridges.

Mode Interface Configuration

Usage notes Interfaces can only be part of one bridge, so when removing the bridge no parameters are required.

Interfaces that have been added to a bridge will lose their Layer 3 properties. The bridge will act as the Layer 3 interface. The bridge will provide Layer 2 connectivity between interfaces that are a part of the same bridge-group.

You can attach interfaces such as Ethernet and VTI (Tunnel) to your bridge.

Examples To add eth0 to bridge 2 in unprotected mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# bridge-group 2
```

To add eth0 to bridge 2 in protected mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# bridge-group 2 port-protected
```

To remove eth0 from bridge 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no bridge-group
```

Related commands

ageing-time

bridge

show bridge

show bridge macaddr

l3-filtering enable

Overview Use this command to enable traffic control for bridged traffic on a bridge interface.

Use the **no** variant of this command to disable traffic control for bridged traffic on a bridge interface.

Syntax

```
l3-filtering enable
no l3-filtering enable
```

Default Traffic control is disabled by default for bridged traffic.

Mode Interface mode for a bridge interface

Example To enable traffic control for bridged traffic on br1, use the commands:

```
awplus# configure terminal
awplus(config)# interface br1
awplus(config-if)# l3-filtering enable
```

Command changes Version 5.4.7-0.1: command added. Previously, traffic control was enabled by default on all bridge interfaces.

mac-learning

Overview Use this command to enable FDB MAC address learning on a bridge interface. In some circumstances, FDB MAC address learning on a software-based router bridge is not useful, and it is better to flood the traffic within interfaces associated with the bridge instance, to ensure the traffic reaches its destination.

Use the **no** variant of this command to disable or enable FDB MAC address learning on a bridge.

Syntax

```
mac-learning
no mac-learning
```

Default Learning is enabled by default.

Mode Interface mode for a bridge interface

Example To turn off learning on bridge 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface br2
awplus(config-if)# no mac-learning
```

To turn learning on bridge 2 back on, use the following commands:

```
awplus# configure terminal
awplus(config)# interface br2
awplus(config-if)# mac-learning
```

Command changes Version 5.4.7-0.1: command added

show bridge

Syntax Use this command to display detailed information about your bridge(s).

Syntax `show bridge [<bridge-list>]`

Parameter	Description
<bridge-list>	The bridge/s to display the information about. The <*bridge-list*> can be: • a single bridge(e.g. br2) • a continuous range of bridges (e.g. br1-3) • a comma separated list of bridges and/or ranges (e.g. br1,br2,br3-br5)

Default Displays detailed information about all bridges, if no <*bridge-list*> is specified.

Mode Privileged Exec

Examples To display information about all bridges, use the following command:

```
awplus#show bridge
```

To display information about bridge 2, use the following command:

```
awplus#show bridge br2
```

To display information about bridge in the range 1 to 3, use the following command:

```
awplus#show bridge br1-3
```

To display information about bridges 1, and from 3 to 5, use the following command:

```
awplus#show bridge br1,br3-5
```

Output Figure 10-1: Example output from the **show bridge** command displaying information about all bridges:

```
awplus#show bridge
Bridge Name     Aging Timer     Interfaces
----------------------------------------
br1             300             eth1
br3             300
br4             300
br5             300
```

Figure 10-2: Example output from the **show bridge** command displaying information about bridge 1.

```
awplus#show bridge br1
Bridge Name     Aging Timer     Interfaces
----------------------------------------
br1             300             eth1
```

Related commands

ageing-time

bridge

bridge-group

show bridge macaddr

show bridge macaddr

Overview Use this command to display the MAC entries learned in the MAC table for your bridge.

Syntax

```
show bridge macaddr <bridge-list>
```

Parameter	Description
<bridge-list>	The bridge interfaces to display the information about. The *<bridge-list>* can be: • a single bridge (e.g. br2) • a continuous range of bridges (e.g. br1-3) • a comma separated list of bridges and/or ranges (e.g. br1,br2,br3-br5)

Mode Global Configuration

Example To display the learned MAC entries for bridge 2, use the following commands:

```
awplus# configure terminal
awplus(config)# show bridge macaddr br2
```

Output Figure 10-3: Example output from the **show bridge macaddr** command displaying information about bridge 2:

```
awplus#show bridge macaddr br2
Bridge Name    Interface    mac addr              is local?  ageing
-----------------------------------------------------------------
br2            eth0         ec:cd:6d:20:c0:fb     no          41
br2            eth0         00:c4:6d:20:c0:e6     no           0
br2            eth0         ec:cd:6d:20:c0:bd     yes          0
...
```

Related commands

ageing-time

bridge

bridge-group

show bridge

11 802.1Q Encapsulation Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure 802.1Q Encapsulation. For more information, see the Interface Feature Overview and Configuration Guide.

Command List

- "encapsulation dot1q" on page 316

encapsulation dot1q

Overview Use this command to enable 802.1Q encapsulation on Ethernet interfaces, L2 tunnel interfaces (e.g. OpenVPN or L2TPv3 Ethernet pseudowire), or the VLAN-aware bridge 0.

Use the **no** variant of this command to disable 802.1Q encapsulation for the VLAN identified by the VLAN ID (VID).

Syntax

```
encapsulation dot1q <vid>
no encapsulation dot1q <vid>
```

Parameter	Description
<vid>	Enter a VLAN ID in the range from 1 through 4094. The VLAN ID identifies the VLAN to which the frames belong. It also identifies the index of the subinterface of the Ethernet interface or Layer 2 tunnel interface.

Default 802.1Q encapsulation is disabled by default on all Ethernet interfaces, Layer 2 tunnel interfaces, and bridge interfaces.

Mode Interface Configuration

Usage notes You should enter the Ethernet interface or tunnel interface configuration mode to enable 802.1Q encapsulation and configure the VID first. Then you can use the VID to configure the sub-interface associated with the Ethernet interface or tunnel interface. Sub-interfaces are logical interfaces. The sub interface index must be the same as the VID. For example, if you configure VID 1 for eth1, then the sub-interface for eth1 is eth1.1. If you configure VID 2 for tunnel20, then the sub-interface for tunnel20 is tunnel20.2.

Examples To enable 802.1Q encapsulation on Ethernet interface eth0, use the commands:

```
awplus# configure terminal
awuplus(config)# interface eth0
awplus(config-if)# encapsulation dot1q 1
```

To enable 802.1Q encapsulation on tunnel interface tunnel20, use the commands:

```
awplus# configure terminal
awuplus(config)# interface tunnel20
awplus(config-if)# encapsulation dot1q 2
```

To enable multiple 802.1Q encapsulation on Ethernet interface eth0, use the commands:

```
awplus# configure terminal
awuplus(config)# interface eth0
awplus(config-if)# encapsulation dot1q 1
awplus(config-if)# encapsulation dot1q 2
awplus(config-if)# encapsulation dot1q 3
```

To disable 802.1Q encapsulation on eth0, use the commands:

```
awplus# configure terminal
awuplus(config)# interface eth0
awuplus(config-if)# no encapsulation dot1q 1
```

Related commands

interface (to configure)

show interface

Part 3: Layer 3 Switching

12 IP Addressing and Protocol Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure various IP features, including the following protocols:

- Address Resolution Protocol (ARP)

For more information, see the IP Feature Overview and Configuration Guide.

Command List

- "arp" on page 321
- "arp log" on page 322
- "arp opportunistic-nd" on page 325
- "arp-loose-check" on page 326
- "clear arp-cache" on page 327
- "debug ip packet interface" on page 328
- "ip address (IP Addressing and Protocol)" on page 330
- "ip forwarding" on page 332
- "ip icmp error-interval" on page 333
- "ip icmp-timestamp" on page 334
- "ip tcp synack-retries" on page 335
- "ip tcp-timestamp" on page 336
- "ip unreachables" on page 337
- "ping" on page 339
- "show arp" on page 340
- "show ip flooding-nexthops" on page 341
- "show ip forwarding" on page 342
- "show ip interface" on page 343

- "show ip sockets" on page 344
- "tcpdump" on page 347
- "traceroute" on page 348
- "undebug ip packet interface" on page 349

arp

Overview This command adds a static ARP entry to the ARP cache. This is typically used to add entries for hosts that do not support ARP or to speed up the address resolution function for a host. The ARP entry must not already exist. Use the **alias** parameter to allow your device to respond to ARP requests for this IP address.

The **no** variant of this command removes the static ARP entry. Use the clear arp-cache command to remove the dynamic ARP entries in the ARP cache.

Syntax

```
arp <ip-addr> <mac-address> [<port-number>] [alias]
no arp <ip-addr>
```

Parameter	Description
<ip-addr>	The IPv4 address of the device you are adding as a static ARP entry.
<mac-address>	The MAC address of the device you are adding as a static ARP entry, in hexadecimal notation with the format HHHH.HHHH.HHHH.
alias	Allows your device to respond to ARP requests for the IP address. Proxy ARP must be enabled on the interface before using this parameter.

Mode Global Configuration

Examples To add the IP address 10.10.10.9 with the MAC address 0010.2533.4566 into the ARP cache, and have your device respond to ARP requests for this address, use the commands:

```
awplus# configure terminal
awplus(config)# arp 10.10.10.9 0010.2533.4566 alias
```

Related commands clear arp-cache

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 IP addresses to physical MAC addresses for hosts.

This command can display the MAC addresses in the ARP log either using the notation HHHH.HHHH.HHHH, or using the IEEE standard hexadecimal notation (HH-HH-HH-HH-HH-HH).

Use the **no** variant of this command to disable the logging of ARP entries.

Syntax

```
arp log [mac-address-format ieee]
no arp log [mac-address-format ieee]
```

Parameter	Description
`mac-address-format ieee`	Display the MAC address in the standard IEEE format (HH-HH-HH-HH-HH-HH), instead of displaying the MAC address with the format HHHH.HHHH.HHHH.

Default The ARP logging feature is disabled by default.

Mode Global Configuration

Usage notes You have the option to change how the MAC address is displayed in the ARP log message. The output can either use the notation HHHH.HHHH.HHHH or HH-HH-HH-HH-HH-HH.

Enter **arp log** to use HHHH.HHHH.HHHH notation.

Enter **arp log mac-address-format ieee** to use HH-HH-HH-HH-HH-HH notation.

Enter **no arp log mac-address-format ieee** to revert from HH-HH-HH-HH-HH-HH to HHHH.HHHH.HHHH.

Enter **no arp log** to disable ARP logging.

To display ARP log messages use the command **show log | include ARP_LOG**.

Examples To enable ARP logging and specify that the MAC address in the log message is displayed in HHHH.HHHH.HHHH notation, use the following commands:

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

To disable ARP logging on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log
```

To enable ARP logging and specify that the MAC address in the log message is displayed in the standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH), use the following commands:

```
awplus# configure terminal
awplus(config)# arp log mac-address-format ieee
```

To leave ARP logging enabled, but stop using HH-HH-HH-HH-HH-HH format and use HHHH.HHHH.HHHH format instead, use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log mac-address-format ieee
```

To display ARP log messages, use the following command:

```
awplus# show log | include ARP_LOG
```

Output Figure 12-1: Output from **show log | include ARP_LOG** after enabling ARP logging using **arp log**. Note that this output uses HHHH.HHHH.HHHH format.

```
awplus#configure terminal
awplus(config)#arp log
awplus(config)#exit
awplus#show log | include ARP_LOG
2022 Mar 6 06:21:01 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 add
0013.4078.3b98 (192.168.2.4)
2022 Mar 6 06:22:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 del
0013.4078.3b98 (192.168.2.4)
2022 Mar 6 06:23:26 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 add
0030.940e.136b (192.168.2.20)
2022 Mar 6 06:23:30 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Figure 12-2: Output from **show log | include ARP_LOG** after enabling ARP logging using **arp log mac-address format ieee**. Note that this output uses HH-HH-HH-HH-HH-HH format.

```
awplus#configure terminal
awplus(config)#arp log mac-address-format ieee
awplus(config)#exit
awplus#show log | include ARP_LOG
2022 Mar 6 06:25:28 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 add
00-17-9a-b6-03-69 (192.168.2.12)
2022 Mar 6 06:25:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 add
00-03-37-6b-a6-a5 (192.168.2.10)
2022 Mar 6 06:26:53 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 del
00-30-94-0e-13-6b (192.168.2.20)
2022 Mar 6 06:27:31 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 del
00-17-9a-b6-03-69 (192.168.2.12)
2022 Mar 6 06:28:09 user.notice awplus HSL[1007]: ARP_LOG port1.0.1 vlan1 del
00-03-37-6b-a6-a5 (192.168.2.10)
2022 Mar 6 06:28:14 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

The following table lists the parameters shown in the output of the **show log | include ARP_LOG** command. The ARP log message format is:

```
<date> <time> <severity> <hostname> <program-name>
ARP_LOG <port-number> <vid> <operation> <MAC> <IP>
```

Table 12-1: Parameters in the output from **show log | include ARP_LOG**

Parameter	Description
ARP_LOG	Indicates that ARP log entry information follows.
<operation>	Indicates "add" if the ARP log entry displays an ARP addition. Indicates "del" if the ARP log entry displays an ARP deletion.
<MAC>	Indicates the MAC address for the ARP log entry, either in the default hexadecimal notation (HHHH.HHHH.HHHH) or in the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) as specified with the **arp log** or the **arp log mac-address-format ieee** command.
<IP>	Indicates the IP address for the ARP log entry.

Related commands

show log

show running-config

arp opportunistic-nd

Overview Use this command to enable opportunistic neighbor discovery for the global ARP cache. This command changes the behavior for unsolicited ARP packet forwarding on the device.

CAUTION: *Opportunistic neighbor discovery can make your device more vulnerable to ARP/ND cache poisoning attacks. We recommend disabling it unless necessary.*

Use the **no** variant of this command to disable opportunistic neighbor discovery for the global ARP cache.

Syntax

```
arp opportunistic-nd
no arp opportunistic-nd
```

Default Opportunistic neighbor discovery is disabled by default.

Mode Global Configuration

Usage notes When opportunistic neighbor discovery is enabled, the device will reply to any received unsolicited ARP packets (but not gratuitous ARP packets). The source MAC address for the unsolicited ARP packet is added to the ARP cache, so the device forwards the ARP packet. When opportunistic neighbor discovery is disabled, the source MAC address for the ARP packet is not added to the ARP cache, so the ARP packet is not forwarded by the device.

Examples To enable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# arp opportunistic-nd
```

To disable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# no arp opportunistic-nd
```

Related commands

ipv6 opportunistic-nd

show arp

show running-config interface

arp-loose-check

Overview Use this command to let AlliedWare Plus process ARPs that have a sender protocol address from outside the interface's local subnets.

Use the **no** variant of this command to return to the default ARP processing behavior. By default, AlliedWare Plus will only process ARP packets that are local to the incoming interface.

Syntax

```
arp-loose-check
no arp-loose-check
```

Default Disabled.

Mode Interface Configuration for Eth, and bridge interfaces and 802.1Q sub-interfaces.

Usage notes By default, AlliedWare Plus will only process ARP packets that are local to the incoming interface, to prevent ARP poisoning. This means the packets must have:

- a sender protocol address inside one of the incoming interface's local subnets, and
- a target protocol address equal to one of the incoming interface's IP addresses.

If you enable loose ARP processing and then use the **no** variant of this command to return to default processing, you may need to clear the ARP cache. Use the clear arp-cache command. This will remove any undesired existing ARPs.

Example To process ARPs that have a sender protocol address from outside eth1's local subnets, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# arp-loose-check
```

To return to the default behavior on eth1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth1
awplus(config-if)# no arp-loose-check
```

Related commands arp

clear arp-cache

show arp

Command changes Version 5.5.2-0.1: command added

clear arp-cache

Overview This command deletes dynamic ARP entries from the ARP cache. You can optionally specify the IPv4 address of an ARP entry to be cleared from the ARP cache.

Syntax

```
clear arp-cache [<ip-address>]
```

Parameter	Description
<ip-address>	The IPv4 address of an ARP entry that is to be cleared from the ARP cache.

Mode Privileged Exec

Usage notes To display the entries in the ARP cache, use the show arp command. To remove static ARP entries, use the no variant of the arp command.

Example To clear all dynamic ARP entries, use the command:

```
awplus# clear arp-cache
```

To clear all dynamic ARP entries associated with the IPv4 address 192.168.1.1, use the command:

```
awplus# clear arp-cache 192.168.1.1
```

Related commands arp

show arp

debug ip packet interface

Overview The **debug ip packet interface** command enables IP packet debug and is controlled by the **terminal monitor** command.

If the optional **icmp** keyword is specified then ICMP packets are shown in the output.

The **no** variant of this command disables the **debug ip packet interface** command.

Syntax

```
debug ip packet interface {<interface-name>|all} [address
<ip-address>|verbose|hex|arp|udp|tcp|icmp]
```

```
no debug ip packet interface [<interface-name>]
```

Parameter	Description
<interface-name>	Specify a single Layer 3 interface name (not a range of interfaces) This keyword can be specified as either all or as a single Layer 3 interface to show debugging for either all interfaces or a single interface.
`all`	Specify all Layer 3 interfaces on the device.
<ip-address>	Specify an IPv4 address. If this keyword is specified, then only packets with the specified IP address as specified in the ip-address placeholder are shown in the output.
`verbose`	Specify **verbose** to output more of the IP packet. If this keyword is specified then more of the packet is shown in the output.
`hex`	Specify **hex** to output the IP packet in hexadecimal. If this keyword is specified, then the output for the packet is shown in hex.
`arp`	Specify **arp** to output ARP protocol packets. If this keyword is specified, then ARP packets are shown in the output.
`udp`	Specify **udp** to output UDP protocol packets. If this keyword is specified then UDP packets are shown in the output.
`tcp`	Specify **tcp** to output TCP protocol packets. If this keyword is specified, then TCP packets are shown in the output.
`icmp`	Specify **icmp** to output ICMP protocol packets. If this keyword is specified, then ICMP packets are shown in the output.

Mode Privileged Exec and Global Configuration

Examples

To turn on ARP packet debugging on eth0, use the command:

```
awplus# debug ip packet interface eth0 arp
```

To turn off IP packet interface debugging on interface eth0, use the command:

```
awplus# no debug ip packet interface eth0
```

To turn on all packet debugging on all interfaces on the device, use the command:

```
awplus# debug ip packet interface all
```

To turn off IP packet interface debugging on all interfaces, use the command:

```
awplus# no debug ip packet interface
```

To turn on TCP packet debugging on eth0 and IP address 192.168.2.4, use the command:

```
awplus# debug ip packet interface eth0 address 192.168.2.4 tcp
```

Related commands

no debug all

tcpdump

terminal monitor

undebug ip packet interface

ip address (IP Addressing and Protocol)

Overview This command sets a static IP address on an interface.

The **no** variant of this command removes the IP address from the interface.

You cannot remove the primary address when a secondary address is present.

Syntax

```
ip address <ip-addr/prefix-length> [secondary] [label <label>]
no ip address [<ip-addr/prefix-length>] [secondary]
```

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length you are assigning to the interface.
`secondary`	Secondary IP address.
`label`	Adds a user-defined description of the secondary IP address.
<label>	A user-defined description of the secondary IP address. Valid characters are any printable character and spaces.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Usage notes To set the primary IP address on the interface, specify only **ip address** *<ip-addr/prefix-length>*. This overwrites any configured primary IP address. To add additional IP addresses on this interface, use the **secondary** parameter. You must configure a primary address on the interface before configuring a secondary address.

NOTE: *Use **show running-config interface**, instead of **show ip interface brief**, when you need to view a secondary address configured on an interface. **show ip interface brief** will only show the primary address, not a secondary address for an interface.*

Examples To add the IP address 10.10.10.50/24 to the interface eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip address 10.10.10.50/24
```

To add the secondary IP address 10.10.11.50/24 to the same interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip address 10.10.11.50/24 secondary
```

To add the IP address 10.10.11.50/24 to the local loopback interface lo, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

To add the IP address 10.10.11.50/24 to the tunnel tunnel0, use the following commands:

Related commands

interface (to configure)

show ip interface

show running-config interface

ip forwarding

Overview This command enables IP forwarding on your device. When enabled, your device routes IP packets.

The **no** variant of this command disables IP forwarding on your device. Even when IP forwarding is not enabled, the device can still work as an IP host; in particular, it can be managed by IP-based applications, such as SNMP, Telnet and SSH.

Syntax

```
ip forwarding
no ip forwarding
```

Default IP forwarding is enabled by default.

Mode Global Configuration

Examples To enable your device to route IP packets, use the commands:

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

To stop your device from routing IP packets, use the commands

```
awplus# configure terminal
awplus(config)# no ip forwarding
```

Related commands show ip forwarding

ip icmp error-interval

Overview Use this command to limit how often IPv4 ICMP error messages are sent. The maximum frequency of messages is specified in milliseconds.

Use the **no** variant of this command to reset the frequency to the default.

Syntax

```
ip icmp error-interval <interval>
no ip icmp error-interval
```

Parameter	Description
<interval>	0-2147483647, interval in milliseconds.

Default 1000

Mode Global Configuration

Example To configure the rate to be at most one packet every 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip icmp error-interval 10000
```

To reset the rate to the default of one packet every second, use the commands:

```
awplus# configure terminal
awplus(config)# no ip icmp error-interval
```

Related commands ipv6 icmp error-interval

ip icmp-timestamp

Overview Use this command to allow ICMP timestamp request and response packets.

Use the **no** variant of this command to drop ICMP timestamp request and response packets.

You may wish to drop these packets because the ICMP timestamp response contains the device's date and time. This information could theoretically be used against some systems to exploit weak time-based random number generators in other services. In addition, it may be possible to fingerprint devices by analyzing their responses to invalid ICMP timestamp requests.

Syntax

```
ip icmp-timestamp
no ip icmp-timestamp
```

Default Allowed

Mode Global Configuration

Example To drop ICMP timestamp packets, use the commands:

```
awplus# configure terminal
awplus(config)# no ip icmp-timestamp
```

To allow ICMP timestamp packets again, use the commands:

```
awplus# configure terminal
awplus(config)# ip icmp-timestamp
```

Related commands ip tcp-timestamp

Command changes Version 5.5.2-0.1: command added

ip tcp synack-retries

Overview Use this command to specify how many times the switch will retry sending a SYN ACK for a TCP connection for which it has received a SYN but not an ACK. Such connections are called half-open TCP connections. This command allows you to influence how long half-open TCP connections take to time out.

Use the **no** variant of this command to return to the default setting of 5 retries.

Syntax

```
ip tcp synack-retries <0-255>
no ip tcp synack-retries
```

Parameter	Description
<0-255>	Number of times to retry sending the SYN ACK

Default 5 retries

Mode Global Configuration

Usage notes The following table shows the approximate correlation between the number of retries and the time half-open TCP connections take to time out.

Number of retries	Approximate lower bound for the timeout
0 retries	1 second
1 retry	3 seconds
2 retries	7 seconds
3 retries	15 seconds
4 retries	31 seconds
5 retries	63 seconds

Example To retry twice, which leads to a timeout of approximately 7 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip tcp synack-retries 2
```

Related commands show running-config

Command changes Version 5.4.7-0.2: command added

ip tcp-timestamp

Overview Use this command to enable TCP timestamp responses.

Use the **no** variant of this command to disable TCP timestamp responses.

You may wish to disable timestamp responses because TCP timestamps may allow other parties to remotely calculate the system uptime and boot time of the device and the device's clock. To prevent this information leaking to potential attackers, we recommend you disable TCP timestamps on the device, unless you need to use them.

Syntax

```
ip tcp-timestamp
no ip tcp-timestamp
```

Default Enabled

Mode Global Configuration

Example To disable TCP timestamp responses, use the commands:

```
awplus# configure terminal
awplus(config)# no ip tcp-timestamp
```

To enable TCP timestamp responses again, use the commands:

```
awplus# configure terminal
awplus(config)# ip tcp-timestamp
```

Related commands ip icmp-timestamp

Command changes Version 5.5.2-0.1: command added

ip unreachables

Overview Use this command to enable ICMP (Internet Control Message Protocol) type 3, destination unreachable, messages.

Use the **no** variant of this command to disable destination unreachable messages. This prevents an attacker from using these messages to discover the topology of a network.

Syntax

```
ip unreachables
no ip unreachables
```

Default Destination unreachable messages are enabled by default.

Mode Global Configuration

Usage notes When a device receives a packet for a destination that is unreachable it returns an ICMP type 3 message, this message includes a reason code, as per the table below. An attacker can use these messages to obtain information regarding the topology of a network. Disabling destination unreachable messages, using the **no ip unreachables** command, secures your network against this type of probing.

NOTE: *Disabling ICMP destination unreachable messages breaks applications such as traceroute and Path MTU Discovery (PMTUD), which depend on these messages to operate correctly.*

Table 12-2: ICMP type 3 reason codes and description

Code	Description [RFC]
0	Network unreachable [RFC792]
1	Host unreachable [RFC792]
2	Protocol unreachable [RFC792]
3	Port unreachable [RFC792]
4	Fragmentation required, and DF flag set [RFC792]
5	Source route failed [RFC792]
6	Destination network unknown [RFC1122]
7	Destination host unknown [RFC1122]
8	Source host isolated [RFC1122]
9	Network administratively prohibited [RFC768]
10	Host administratively prohibited [RFC869]
11	Network unreachable for Type of Service [RFC908]
12	Host unreachable for Type of Service [RFC938]
13	Communication administratively prohibited [RFC905]

Table 12-2: ICMP type 3 reason codes and description (cont.)

Code	Description [RFC]
14	Host Precedence Violation [RFC1812]
15	Precedence cutoff in effect [RFC1812]

Example To disable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# no ip unreachables
```

To enable destination unreachable messages, use the commands

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

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 the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show arp
```

Mode User Exec and Privileged Exec

Usage notes Running this command with no additional parameters will display all entries in the ARP routing and forwarding table.

Example To display all ARP entries in the ARP cache, use the following command:

```
awplus# show arp
```

Output Figure 12-3: Example output from the **show arp** command

```
awplus#show arp
IP Address       LL Address        Interface  Port          Type
192.168.3.2      0000.cd37.04de    eth0.3     -             dynamic
10.34.180.4      0800.278c.aaba    eth0.1034  -             dynamic
10.34.180.254    eccd.6d41.e8f1    eth0.1034  -             dynamic
192.168.2.2      eccd.6dd0.c136    eth0.2     -             dynamic
```

Table 13: Parameters in the output of the **show arp** command

Parameter	Meaning
IP Address	IP address of the network device this entry maps to.
LL Address	Hardware address of the network device.
Interface	Interface over which the network device is accessed.
Port	Physical port that the network device is attached to.
Type	Whether the entry is a static or dynamic entry. Static entries are added using the arp command. Dynamic entries are learned from ARP request/reply message exchanges.

Related commands

arp

clear arp-cache

Command changes Version 5.4.9-0.1: Link layer addresses now shown as the hardware address (MAC Address output parameter has been renamed to LL Address).

show ip flooding-nexthops

Overview Use this command to display the static and dynamic ARP entries in the ARP cache that flood packets to multiple ports.

Syntax

```
show ip flooding-nexthops
```

Mode User Exec and Privileged Exec

Example To display all of the flooding nexthop entries in the ARP cache, use the command:

```
awplus# show ip flooding-nexthops
```

Output Figure 12-4: Example output from **show ip flooding-nexthops**

```
awplus#show ip flooding-nexthops
IP Address      MAC Address     Interface         Flooding Mode    Type
11.11.11.10     0300.0000.0011  eth0              port-group       static
```

Related commands show arp

Command changes Version 5.4.8-2.1: command added

show ip forwarding

Overview Use this command to display the IP forwarding status.

Syntax

```
show ip forwarding
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ip forwarding
```

Output Figure 12-5: Example output from the **show ip forwarding** command

```
awplus#show ip forwarding
IP forwarding is on
```

Related commands ip forwarding

show ip interface

Overview Use this command to display information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip interface [<interface-list>] [brief]
```

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the **encapsulation dot1q** command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. The specified interfaces must exist.

Mode User Exec and Privileged Exec

Examples To show the IP addresses assigned to eth0, use the command:

```
awplus# show ip interface eth0 brief
```

Output Figure 12-6: Example output from the **show ip interface brief** command

```
Interface               IP-Address          Status          Protocol
eth0                    unassigned          admin up        running
eth0.3                  192.168.3.1/24      admin up        running
eth0.2                  192.168.2.1/24      admin up        running
lo                      unassigned          admin up        running
br0                     unassigned          admin up        down
```

show ip sockets

Overview Use this command to display information about the IP or TCP sockets that are present on the device. It includes TCP and UDP listen sockets, and displays the associated IP address and port.

The information displayed for established TCP sessions includes the remote IP address, port, and session state. Raw IP protocol listen socket information is also displayed for protocols such as ICMP6, which are configured to receive IP packets with the associated protocol number.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip sockets
```

Mode Privileged Exec

Usage notes Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Note that this command does not display sockets that are used internally for exchanging data between the various processes that exist on the device and are involved in its operation and management. It only displays sockets that are present for the purposes of communicating with other external devices.

Example To display IP sockets currently present on the device, use the command:

```
awplus# show ip sockets
```

Output Figure 12-7: Example output from **show ip sockets**

```
Socket information

Not showing 40 local connections
Not showing 7 local listening ports

Typ Local Address           Remote Address          State
tcp 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp 0.0.0.0:4743            0.0.0.0:*               LISTEN
tcp 0.0.0.0:873             0.0.0.0:*               LISTEN
tcp :::23                   :::*                    LISTEN
udp 0.0.0.0:111             0.0.0.0:*
udp 226.94.1.1:5405         0.0.0.0:*
udp 0.0.0.0:161             0.0.0.0:*
udp :::161                  :::*
raw 0.0.0.0:112             0.0.0.0:*               112
raw :::58                   :::*                    58
raw :::112                  :::*                    112
```

Table 12-1: Parameters in the output from **show ip sockets**

Parameter	Description
`Not showing <number> local connections`	This field refers to established sessions between processes internal to the device, that are used in its operation and management. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.
`Not showing <number> local listening ports`	This field refers to listening sockets belonging to processes internal to the device, that are used in its operation and management. They are not available to receive data from other devices. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.
`Typ`	This column displays the type of the socket. Possible values for this column are: `tcp` : IP Protocol 6 `udp` : IP Protocol 17 `raw` : Indicates that socket is for a non port-orientated protocol (i.e. a protocol other than TCP or UDP) where all packets of a specified IP protocol type are accepted. For raw socket entries the protocol type is indicated in subsequent columns.
`Local Address`	For TCP and UDP listening sockets this shows the destination IP address and destination TCP or UDP port number for which the socket will receive packets. The address and port are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 or :: for IPv6. For active TCP sessions the IP address will display which of the devices addresses the session was established with. For raw sockets this displays the IP address and IP protocol for which the socket will accept IP packets. The address and protocol are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 and :: for IPv6. IP Protocol assignments are described at:www.iana.org/assignments/protocol-numbers

Table 12-1: Parameters in the output from **show ip sockets** (cont.)

Parameter	Description
`Remote Address`	For TCP and UDP listening sockets this shows the source IP address (either IPv4 or IPv6) and source TCP or UDP port number for which the socket will accept packets. The address and port are separated by ':'. If the socket will accept packets addressed from any IP address, the IP address will be 0.0.0.0 for IPv4 . This is the usual case for a listening socket. Normally for a listen socket any source port will be accepted. This is indicated by ". For active TCP sessions the IP address will display the remote address and port the session was established with. For raw sockets the entry in this column will be 0.0.0.0: for IPv4 .

`State`	This column shows the state of the socket. For TCP sockets this shows the state of the TCP state machine. For UDP sockets this column is blank. For raw sockets it contains the IP protocol number. The possible TCP states are:
	`LISTEN`
	`SYN-SENT`
	`SYN-RECEIVED`
	`ESTABLISHED`
	`FIN-WAIT-1`
	`FIN-WAIT-2`
	`CLOSE-WAIT`
	`CLOSING`
	`LAST-ACK`
	`TIME-WAIT`
	`CLOSED`
	RFC793 contains the TCP state machine diagram with Section 3.2 describing each of the states.

tcpdump

Overview Use this command to start a tcpdump, which gives the same output as the Unix-like **tcpdump** command to display TCP/IP traffic. Press `<ctrl> + c` to stop a running tcpdump.

Syntax `tcpdump <line>`

Parameter	Description
<line>	Specify the dump options. For more information on the options for this placeholder see http://www.tcpdump.org/tcpdump_man.html

Mode Privileged Exec

Example To start a tcpdump running to capture IP packets, enter the command:

```
awplus# tcpdump ip
```

Output Figure 12-8: 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
<ip-addr>	The destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<hostname>	The destination hostname.

Mode User Exec and Privileged Exec

Example

```
awplus# traceroute 10.10.0.5
```

undebug ip packet interface

Overview This command applies the functionality of the no debug ip packet interface command.

13 Domain Name Service (DNS) Commands

Introduction

Overview This chapter provides an alphabetical reference of Domain Name Service (DNS) commands.

Command List

- "ip dns forwarding domain-list" on page 351
- "ip domain-list" on page 352
- "ip domain-lookup" on page 353
- "ip domain-name" on page 354
- "ip name-server" on page 355
- "show hosts" on page 357
- "show ip domain-list" on page 358
- "show ip domain-name" on page 359
- "show ip name-server" on page 360

ip dns forwarding domain-list

Overview Use this command to create a domain-list that can be used as a suffix-list for DNS lookups. This command puts the device into a new mode where subsequent commands can be entered. The new mode is "Domain List Configuration" mode.

Use the **no** variant of this command to delete the domain-list.

Syntax

```
ip dns forwarding domain-list <domain-list-name>
no ip dns forwarding domain-list <domain-list-name>
```

Parameter	Description
<domain-list-name>	Name of the list.

Mode Global Configuration

Usage notes The domain list can be used by features that need to match against domains. A domain list by itself does nothing; it must be attached to another feature to have functionality (like a prefix-list). For example, the domain list can be used as a suffix list on an DNS name-server. The DNS server can be either statically configured, or learned over a PPP connection.

Note that this command is separate from the **ip domain-list** command, which is used by DNS client to append a domain on to the end of a partial hostname to form a fully-qualified domain.

Examples To create a domain list to include domains that are internal to the company such as "engineering.acme" or "intranet.acme", use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding domain-list corporatedomains
awplus(config-domain-list)# description internal network domain
awplus(config-domain-list)# domain engineering.acme
awplus(config-domain-list)# domain intranet.acme
```

To delete the domain list, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding domain-list
corporatedomains
```

Related commands ip name-server

ip domain-list

Overview This command adds a domain to the DNS list. Domains are appended to incomplete host names in DNS requests. Each domain in this list is tried in turn in DNS lookups. This list is ordered so that the first entry you create is checked first.

The **no** variant of this command deletes a domain from the list.

Syntax

```
ip domain-list <domain-name>
no ip domain-list <domain-name>
```

Parameter	Description
<domain-name>	Domain string, for example “company.com”.

Mode Global Configuration

Usage notes If there are no domains in the DNS list, then your device uses the domain specified with the ip domain-name command. If any domain exists in the DNS list, then the device does not use the domain set using the **ip domain-name** command.

Example To add the domain `example.net` to the DNS list, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-list example.net
```

Related commands

ip domain-lookup

ip domain-name

show ip domain-list

ip domain-lookup

Overview This command enables the DNS client on your device. This allows you to use domain names instead of IP addresses in commands. The DNS client resolves the domain name into an IP address by sending a DNS inquiry to a DNS server, specified with the ip name-server command.

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 notes The client is enabled by default. However, it does not attempt DNS inquiries unless there is a DNS server configured.

Examples To enable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup
```

To 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

Command changes Version 5.4.8-1.1: via-relay parameter added

ip domain-name

Overview This command sets a default domain for the DNS. The DNS client appends this domain to incomplete host-names in DNS requests.

The **no** variant of this command removes the domain-name previously set by this command.

Syntax

```
ip domain-name <domain-name>
no ip domain-name <domain-name>
```

Mode Global Configuration

Usage notes If there are no domains in the DNS list (created using the ip domain-list command) then your device uses the domain specified with this command. If any domain exists in the DNS list, then the device does not use the domain configured with this command.

When your device is using its DHCP client for an interface, it can receive Option 15 from the DHCP server. This option replaces the domain name set with this command.

Example To configure the domain name, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-name company.com
```

Related commands

ip domain-list

show ip domain-list

show ip domain-name

ip name-server

Overview Use this command to add IPv4 or IPv6 DNS server addresses. The DNS client on your device sends DNS queries to IP addresses in this list when trying to resolve a host name. Host names cannot be resolved until you have added at least one server to this list. A maximum of three name servers can be added to this list.

The **no** variant of this command removes the specified DNS name-server address.

Parameter	Description
<ip-addr>	The IP address of the DNS server that is being added to the name server list. The address is entered in the form A.B.C.D for an IPv4 address, or in the form X:X::X:X for an IPv6 address. The order that you enter the servers in, is the order in which they will be used.

Mode Global Configuration

Usage notes To allow the device to operate as a DNS proxy, your device must have learned about a DNS name-server to forward requests to. Name-servers can be learned through the following means:

- Manual configuration, using the **ip name-server** command
- Learned from DHCP server with Option 6

Use this command to statically configure a DNS name-server for the device to use.

The order that you enter the servers in, is the order in which they will be used.

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 dns forwarding domain-list

ip domain-list

ip domain-lookup

ip domain-name

show ip name-server

Command changes Version 5.4.6-2.1: VRF-lite support added to AR-series devices.

show hosts

Overview This command shows the default domain, domain list, and name servers configured on your device.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show hosts
```

Mode User Exec and Privileged Exec

Example To display the default domain, use the command:

```
awplus# show hosts
```

Output Figure 13-1: Example output from the **show hosts** command when **no ip domain-lookup** is configured

```
awplus#show hosts

Default domain is not set
Name/address lookup is disabled
```

Figure 13-2: Example output from the **show hosts** command when **ip domain-lookup** is configured

```
awplus#show hosts

Default domain is mycompany.com
Domain list: company.com
Name/address lookup uses domain service
Name servers are 10.10.0.2 10.10.0.88
```

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 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 13-3: Example output from the **show ip domain-list** command

```
awplus#show ip domain-list
alliedtelesis.com
mycompany.com
```

Related commands ip domain-list

ip domain-lookup

show ip domain-name

Overview This command shows the default domain configured on your device. When there are no entries in the DNS list, the DNS client appends this domain to incomplete hostnames when sending a DNS inquiry to a DNS server.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show ip domain-name
```

Mode User Exec and Privileged Exec

Example To display the default domain configured on your device, use the command:

```
awplus# show ip domain-name
```

Output Figure 13-4: Example output from the **show ip domain-name** command

```
awplus#show ip domain-name
alliedtelesis.com
```

Related commands ip domain-name

ip domain-lookup

show ip name-server

Overview This command displays a list of IPv4 and IPv6 DNS server addresses that your device will send DNS requests to. This is a static list configured using the ip name-server command.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip name-server
```

Mode User Exec and Privileged Exec

Example To display the list of DNS servers that your device sends DNS requests to, use the command:

```
awplus# show ip name-server
```

Output Figure 13-5: 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

14 IPv6 Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure IPv6. For more information, see the IPv6 Feature Overview and Configuration Guide.

Command List

- "clear ipv6 neighbors" on page 363
- "ipv6 address" on page 364
- "ipv6 address autoconfig" on page 365
- "ipv6 address suffix" on page 367
- "ipv6 enable" on page 368
- "ipv6 eui64-linklocal" on page 370
- "ipv6 forwarding" on page 371
- "ipv6 icmp error-interval" on page 372
- "ipv6 nd accept-ra-default-routes" on page 373
- "ipv6 nd accept-ra-pinfo" on page 374
- "ipv6 nd current-hoplimit" on page 375
- "ipv6 nd dns search-list" on page 376
- "ipv6 nd dns-server" on page 377
- "ipv6 nd managed-config-flag" on page 378
- "ipv6 nd minimum-ra-interval" on page 379
- "ipv6 nd other-config-flag" on page 380
- "ipv6 nd prefix" on page 381
- "ipv6 nd ra-interval" on page 383
- "ipv6 nd ra-lifetime" on page 384

- "ipv6 nd reachable-time" on page 385
- "ipv6 nd retransmission-time" on page 386
- "ipv6 nd route-information" on page 387
- "ipv6 nd router-preference" on page 388
- "ipv6 nd suppress-ra" on page 389
- "ipv6 opportunistic-nd" on page 390
- "ipv6 route" on page 391
- "ipv6 unreachables" on page 393
- "ping ipv6" on page 394
- "show ipv6 forwarding" on page 396
- "show ipv6 interface" on page 397
- "show ipv6 neighbors" on page 398
- "show ipv6 route" on page 399
- "show ipv6 route summary" on page 401
- "traceroute ipv6" on page 402

clear ipv6 neighbors

Overview Use this command to clear all dynamic IPv6 neighbor entries.

Syntax
```
clear ipv6 neighbors
```

Mode Privileged Exec

Example
```
awplus# clear ipv6 neighbors
```

Related commands show ipv6 neighbors

ipv6 address

Overview Use this command to set the IPv6 address of an interface. The command also enables IPv6 on the interface, which creates an EUI-64 link-local address as well as enabling RA processing and SLAAC.

To stop the device from processing prefix information (routes and addresses from the received Router Advertisements) use the command **no ipv6 nd accept-ra-pinfo**.

To remove the EUI-64 link-local address, use the command **no ipv6 eui64-linklocal**.

Use the **no** variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

Syntax

```
ipv6 address <ipv6-addr/prefix-length>
no ipv6 address <ipv6-addr/prefix-length>
```

Parameter	Description
<ipv6-addr/prefix-length>	Specifies the IPv6 address to be set. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Examples To assign the IPv6 address 2001:0db8::a2/64 to eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

Related commands

ipv6 address autoconfig

ipv6 enable

ipv6 eui64-linklocal

show running-config

show ipv6 interface

ipv6 address autoconfig

Overview Use this command to enable IPv6 stateless address autoconfiguration (SLAAC) for an interface. This configures an IPv6 address on an interface derived from the MAC address on the interface.

Use the **no** variant of this command to disable IPv6 SLAAC on an interface. Note that if no global addresses are left after removing all IPv6 autoconfigured addresses then IPv6 is disabled.

Syntax

```
ipv6 address autoconfig
no ipv6 address autoconfig
```

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Usage notes Use this command to enable automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface, and enable IPv6.

IPv6 hosts can configure themselves when connected to an IPv6 network using ICMPv6 (Internet Control Message Protocol version 6) router discovery messages. Configured routers respond with a Router Advertisement (RA) containing configuration parameters for IPv6 hosts.

The SLAAC process derives the interface identifier of the IPv6 address from the MAC address of the interface.

Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them. See the ipv6 enable command for more information.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the ipv6 enable command then it will not be removed using a **no ipv6 address** command.

Examples To enable SLAAC on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 address autoconfig
```

To disable SLAAC on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 address autoconfig
```

Related commands

ipv6 address

ipv6 enable

show ipv6 interface

show running-config

ipv6 address suffix

Overview Use this command to configure the suffix to use when generating an address from prefix information. Any addresses that were created with the EUI-64 suffix will be removed, and new addresses will be added after the next Router Advertisement.

Use the **no** variant of this command to set it back to the default of disabled or set to :: for the same result as the **no** variant.

Syntax

```
ipv6 address suffix <ipv6-addr-suffix>
no ipv6 address suffix
```

Parameter	Description
<ipv6-addr-suffix>	In the format of ::X:X:X:X, for example ::a2d8:0fd8

Default Disabled

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Example To configure the suffix to use when generating an address from prefix information on eth0, use the command:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 address suffix ::a2d8:0fd8
```

Related commands ipv6 nd accept-ra-pinfo

show running-config interface

Command changes Version 5.4.8-2.1: command added

ipv6 enable

Overview Use this command to enable automatic configuration of a link-local IPv6 address on an interface using Stateless Automatic Address Configuration (SLAAC). By default, the EUI-64 method is used to generate the link-local address.

Use the **no** variant of this command to disable IPv6 on an interface without a global address. Note, to stop EUI-64 from generating the automatic link-local address, use the command **no ipv6 eui64-linklocal**.

Syntax

```
ipv6 enable
no ipv6 enable
```

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Usage notes The **ipv6 enable** command automatically configures an IPv6 link-local address on the interface and enables the interface for IPv6 processing.

A link-local address is an IP (Internet Protocol) address that is only used for communications in the local network, or for a point-to-point connection. Routing does not forward packets with link-local addresses. IPv6 requires that a link-local address is assigned to each interface that has the IPv6 protocol enabled, and when addresses are assigned to interfaces for routing IPv6 packets.

Note that the device keeps link-local addresses until you remove them with the **no** variant of the command that established them.

Also note that the device keeps the link-local address if the global address is removed using a command other than the command that was used to establish the link-local address. For example, if a link local address is established with the ipv6 enable command then it will not be removed using a **no ipv6 address** command.

Default All interfaces default to IPv6-down with no address.

Examples To enable IPv6 with only a link-local IPv6 address on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 enable
```

Related commands

ipv6 address

ipv6 address autoconfig

show ipv6 interface

show running-config

ipv6 eui64-linklocal

Overview When IPv6 is enabled on an interface, an EUI link-local address is generated and installed on the interface. In other words, **ipv6 eui64-linklocal** is enabled by default on any IPv6 enabled interface.

Use the **no** variant of this command to disallow the automatic generation of the EUI-64 link-local address on an IPv6 enabled interface.

Syntax

```
ipv6 eui64-linklocal
no ipv6 eui64-linklocal
```

Default The command **ipv6 eui64-linklocal** is enabled by default on any IPv6 enabled interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Example To enable IPv6 on an interface eth0, and use the link-local address of fe80::1/10 instead of the EUI-64 link-local that is automatically generated, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
awplus(config-if)# no ipv6 eui64-linklocal
awplus(config-if)# ipv6 address fe80::1/10
```

Related commands

ipv6 address

ipv6 address autoconfig

ipv6 enable

Command changes Version 5.4.7-0.1: command added

ipv6 forwarding

Overview Use this command to turn on IPv6 unicast routing for IPv6 packet forwarding.

Use this command globally on your device before using the ipv6 enable command on individual interfaces.

Use the **no** variant of this command to turn off IPv6 unicast routing. Note IPv6 unicast routing is disabled by default.

Syntax

```
ipv6 forwarding
no ipv6 forwarding
```

Mode Global Configuration

Default IPv6 unicast forwarding is disabled by default.

Usage notes Enable IPv6 unicast forwarding globally for all interfaces on your device with this command. Use the **no** variant of this command to disable IPv6 unicast forwarding globally for all interfaces on your device.

IPv6 unicast forwarding allows devices to communicate with devices that are more than one hop away, providing that there is a route to the destination address. If IPv6 forwarding is not enabled then pings to addresses on devices that are more than one hop away will fail, even if there is a route to the destination address.

Examples To enable IPv6 unicast routing, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
```

To disable IPv6 unicast routing, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 forwarding
```

Related commands ipv6 enable

ipv6 icmp error-interval

Overview Use this command to limit how often IPv6 ICMP error messages are sent. The maximum frequency of messages is specified in milliseconds.

Use the **no** variant of this command to reset the frequency to the default

Syntax

```
ipv6 icmp error-interval <interval>
no ipv6 icmp error-interval
```

Parameter	Description
<interval>	0-2147483647, interval in milliseconds.

Default 1000

Mode Global Configuration

Example To configure the rate to be at most one packet every 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 icmp error-interval 10000
```

To reset the rate to the default of one packet every second, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 icmp error-interval
```

Related commands ip icmp error-interval

ipv6 nd accept-ra-default-routes

Overview Use this command to allow accepting and installing of default routes based on a received RA (Router Advertisement). The default route's destination is set to the source address of the received RA.

Use the **no** variant of this command to disable accepting RA-based default routes.

Syntax

```
ipv6 nd accept-ra-default-routes
no ipv6 nd accept-ra-default-routes
```

Default RA-based default routes are accepted by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Example To enable RA-based default routes on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd accept-ra-default-routes
```

Related commands

ipv6 address

ipv6 address autoconfig

ipv6 enable

ipv6 nd accept-ra-pinfo

Overview Use this command to allow the processing of the prefix information included in a received RA (Router Advertisement) on an IPv6 enabled interface.

Use the **no** variant of this command to disable an IPv6 interface from using the prefix information within a received RA.

Syntax
```
ipv6 nd accept-ra-pinfo
no ipv6 nd accept-ra-pinfo
```

Default The command **ipv6 nd accept-ra-pinfo** is enabled by default on any IPv6 interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Usage notes By default, when IPv6 is enabled on an interface, SLAAC is also enabled. SLAAC addressing along with the EUI-64 process, uses the prefix information included in a received RA to generate an automatic link-local address on the IPv6 interface.

Note: an AlliedWare Plus device will, by default, add a prefix for the connected interface IPv6 address(es) to the RA it transmits. However, this behavior can be changed by using the command **no ipv6 nd prefix auto-advertise**, so there is no guarantee that an RA will contain a prefix.

Example To enable IPv6 on eth0 without installing a SLAAC address on the interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
awplus(config-if)# no ipv6 nd accept-ra-pinfo
```

Related commands
ipv6 address
ipv6 address autoconfig
ipv6 enable

Command changes Version 5.4.7-0.1: command added

ipv6 nd current-hoplimit

Overview Use this command to specify the advertised current hop limit used between IPv6 Routers.

Use the **no** variant of this command to reset the current advertised hop limit to the default of 0, which means no advertised current hop limit is specified.

Syntax

```
ipv6 nd current-hoplimit <hoplimit>
no ipv6 nd current-hoplimit
```

Parameter	Description
<hoplimit>	Specifies the advertised current hop limit value. Valid values are from 0 to 255 hops.

Default 0 (No advertised current hop limit specified)

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Examples To set the advertised current hop limit to 2 between IPv6 Routers on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd current-hoplimit 2
```

To reset the advertised current hop limit to the default 0 on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd current-hoplimit
```

Related commands

ipv6 nd managed-config-flag

ipv6 nd prefix

ipv6 nd suppress-ra

ipv6 nd dns search-list

Overview Use this command to specify a DNS Search List (DNSSL) to be included in the Router Advertisment for a given IPv6 interface.

Use the **no** variant of this command to remove a specified domain name. If no domain name is specified, then all domain names previously added will be deleted.

Syntax

```
ipv6 nd dns search-list <domain-name>
no ipv6 nd dns search-list [<domain-name>]
```

Parameter	Description
<domain-name>	A string specifying the domain name to be added to the search list. For example, myexample.com

Default No domain search list is included in router advertisements from any interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Example To add the domain name 'myexample.com' to the search list for eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd dns search-list myexample.com
```

To delete all domain names added previously, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd dns search-list
```

Related commands ipv6 nd suppress-ra

Command changes Version 5.5.0-2.5: command added

ipv6 nd dns-server

Overview Use this command to advertise (in Router Advertisement messages) a DNS server for downstream devices to use.

Use the **no** variant of this command to delete one or all DNS server addresses.

Syntax

```
ipv6 nd dns-server <ip-add>
no ipv6 nd dns-server [<ip-add>]
```

Parameter	Description
<ip-add>	Advertise a particular IPv6 address as a DNS server for downstream devices.

Default No DNS servers are advertised.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Example To configure eth0 to send RAs and advertise 2001:DB8::2 as a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd suppress-ra
awplus(config-if)# no ipv6 nd accept-ra-pinfo
awplus(config-if)# ipv6 address 2001:DB8::1/64
awplus(config-if)# ipv6 nd dns-server 2001:DB8::2
```

To stop advertising any DNS servers on the selected interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd dns-server
```

Related commands

ipv6 nd accept-ra-pinfo

ipv6 nd suppress-ra

show ipv6 interface

ipv6 nd managed-config-flag

Overview Use this command to set the managed address configuration flag, contained within the router advertisement field.

Setting this flag indicates the operation of a stateful autoconfiguration protocol such as DHCPv6 for address autoconfiguration, and that address information (i.e. the network prefix) and other (non-address) information can be requested from the device.

An unset flag enables hosts receiving the advertisements to use a stateless autoconfiguration mechanism to establish their IPv6 addresses. The default is flag unset.

Use the **no** variant of this command to reset this command to its default of having the flag unset.

Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

Default Unset

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Usage notes To enable the transmission of router advertisements, you must apply the **no** version of the ipv6 nd suppress-ra command. This step is included in the example below.

Example To set the managed address configuration flag on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd managed-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

Related commands

ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd other-config-flag

ipv6 nd minimum-ra-interval

Overview Use this command in Interface Configuration mode to set a minimum Router Advertisement (RA) interval for an interface.

Use the **no** variant of this command in Interface Configuration mode to remove the minimum RA interval for an interface.

Syntax

```
ipv6 nd minimum-ra-interval <seconds>
no ipv6 nd minimum-ra-interval
```

Parameter	Description
<seconds>	Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 3 to 1350 seconds.

Default The RA interval for an interface is unset by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Examples To set the minimum RA interval for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd minimum-ra-interval 60
```

To remove the minimum RA interval for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd minimum-ra-interval
```

Related commands

ipv6 nd ra-interval

ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd other-config-flag

ipv6 nd other-config-flag

Overview Use this command to set the **other** stateful configuration flag (contained within the router advertisement field) to be used for IPv6 address auto-configuration. This flag is used to request the router to provide information in addition to providing addresses.

Setting the ipv6 nd managed-config-flag command implies that the ipv6 nd other-config-flag will also be set.

Use **no** variant of this command to reset the value to the default.

Syntax

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

Default Unset

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Usage notes To enable the transmission of router advertisements, you must apply the **no** version of the ipv6 nd suppress-ra command. This step is included in the example below.

Example To set the IPv6 other-config-flag on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd other-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

Related commands

ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd managed-config-flag

ipv6 nd prefix

Overview Use this command in Interface Configuration mode to specify the IPv6 prefix information that is advertised by the router advertisement for IPv6 address auto-configuration.

Use the **no** parameter with this command to reset the IPv6 prefix for an interface in Interface Configuration mode.

Syntax

```
ipv6 nd prefix <ipv6-prefix/length>
ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime>
ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime>
<preferred-lifetime> [no-autoconfig]
ipv6 nd prefix <ipv6-prefix/length> <valid-lifetime>
<preferred-lifetime> off-link [no-autoconfig]
no ipv6 nd prefix [<ipv6-addr/prefix-length>|all]
```

Parameter	Description
<ipv6-prefix/length>	The prefix to be advertised by the router advertisement message. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64. The default is X:X::/64.
<valid-lifetime>	The the period during which the specified IPv6 address prefix is valid. This can be set to a value between 0 and 4294967295 seconds. The default is 2592000 (30 days). Note that this period should be set to a value greater than that set for the prefix preferred-lifetime.
<preferred-lifetime>	Specifies the IPv6 prefix preferred lifetime. This is the period during which the IPv6 address prefix is considered a current (undeprecated) value. After this period, the command is still valid but should not be used in new communications. Set to a value between 0 and 4294967295 seconds. The default is 604800 seconds (7 days). Note that this period should be set to a value less than that set for the prefix valid-lifetime.
`off-link`	Specify the IPv6 prefix off-link flag. The default is flag set.
`no-autoconfig`	Specify the IPv6 prefix no autoconfiguration flag. Setting this flag indicates that the prefix is not to be used for autoconfiguration. The default is flag set.
`all`	Specify all IPv6 prefixes associated with the interface.

Default Valid-lifetime default is 2592000 seconds (30 days). Preferred-lifetime default is 604800 seconds (7 days).

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Usage notes This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

Examples To configure the device to issue router advertisements on eth0, and advertise the address prefix of 2001:0db8::/64, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64
```

To configure the device to issue router advertisements on eth0, and advertise the address prefix of 2001:0db8::/64 with a valid lifetime of 10 days and a preferred lifetime of 5 days, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
```

To configure the device to issue router advertisements on eth0 and advertise the address prefix of 2001:0db8::/64 with a valid lifetime of 10 days, a preferred lifetime of 5 days, and no prefix used for autoconfiguration, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
no-autoconfig
```

To reset router advertisements on eth0, so the address prefix of 2001:0db8::/64 is not advertised from the device, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/64
```

To reset all router advertisements on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd prefix all
```

Related commands ipv6 nd suppress-ra

ipv6 nd ra-interval

Overview Use this command to specify the interval between IPv6 Router Advertisements (RA) transmissions.

Use **no** parameter with this command to reset the value to the default value (600 seconds).

Syntax

```
ipv6 nd ra-interval <seconds>
no ipv6 nd ra-interval
```

Parameter	Description
<seconds>	Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 4 to 1800 seconds.

Default 600 seconds.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Usage notes To enable the transmission of router advertisements, you must apply the **no** version of the ipv6 nd suppress-ra command. This step is included in the example below.

Example To set the advertisements interval on eth0 to be 60 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd ra-interval 60
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the advertisements interval on eth0 to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd ra-interval
```

Related commands

ipv6 nd minimum-ra-interval

ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd ra-lifetime

Overview Use this command to specify the time period that this router can usefully act as a default gateway for the network. Each router advertisement resets this time period.

Use **no** parameter with this command to reset the value to default.

Syntax

```
ipv6 nd ra-lifetime <seconds>
no ipv6 nd ra-lifetime
```

Parameter	Description
<seconds>	Time period in seconds. Valid values are from 0 to 9000. Note that you should set this time period to a value greater than the value you have set using the ipv6 nd ra-interval command.

Default 1800 seconds

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Usage notes This command specifies the lifetime of the current router to be announced in IPv6 Router Advertisements.

To enable the transmission of router advertisements, you must apply the **no** version of the ipv6 nd suppress-ra command. This step is included in the example below.

Examples To set the advertisement lifetime of 8000 seconds on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd ra-lifetime 8000
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the advertisement lifetime to the default on eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd ra-lifetime
```

Related commands ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd reachable-time

Overview Use this command to specify the reachable time in the router advertisement to be used for detecting reachability of the IPv6 neighbor.

Use the **no** variant of this command to reset the value to default.

Syntax

```
ipv6 nd reachable-time <milliseconds>
no ipv6 nd reachable-time
```

Parameter	Description
<milliseconds>	Time period in milliseconds. Valid values are from 1000 to 3600000. Setting this value to 0 indicates an unspecified reachable-time.

Default 0 milliseconds

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Usage notes This command specifies the reachable time of the current router to be announced in IPv6 Router Advertisements.

To enable the transmission of router advertisements, you must apply the **no ipv6 nd suppress-ra** command. This instruction is included in the example shown below.

Example To set the reachable-time in router advertisements on eth0 to be 1800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd reachable-time 1800000
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the reachable-time in router advertisements on eth0 to an unspecified reachable-time (0 milliseconds), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd reachable-time
```

Related commands ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd retransmission-time

Overview Use this command to specify the advertised retransmission interval for Neighbor Solicitation in milliseconds between IPv6 Routers.

Use the **no** variant of this command to reset the retransmission time to the default (1 second).

Syntax

```
ipv6 nd retransmission-time <milliseconds>
no ipv6 nd retransmission-time
```

Parameter	Description
<milliseconds>	Time period in milliseconds. Valid values are from 1000 to 3600000.

Default 1000 milliseconds (1 second)

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Examples To set the retransmission-time of Neighbor Solicitation on eth0 to be 800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd retransmission-time 800000
```

To reset the retransmission-time of Neighbor Solicitation on eth0 to the default 1000 milliseconds (1 second), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd retransmission-time
```

Related commands ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd route-information

Overview Use this command to supply more specific route information to be included in the RA (Router Advertisement) the device sends to downstream devices on the same link/LAN.

Use the **no** variant of this command to remove some or all route information.

Syntax

```
ipv6 nd route-information <ipv6-prefix/length>
[<0-4294967295>|infinity|default] [low|medium|high]
ipv6 nd route-information <ipv6-prefix/length>
no ipv6 nd route-information <ipv6-prefix/length>
no ipv6 nd route-information all
```

Parameter	Description
<ipv6-prefix/length>	The IPv6 network prefix and prefix length entered in dotted decimal format for the IPv6 network prefix, then slash notation for the IPv6 prefix length in the format X:X::X:X/ M, e.g. 2001:db8::/64
<0-4294967295>|infinity|default	The length of time in seconds (relative to the time the packet is sent) that the prefix is valid for route determination. • infinity - specifies that the route advertisement has an infinite lifetime. • default - is 3 * MaxRtrAdvInterval
low|medium|high	The preference value for the route information

Default No route information option is included in router advertisement on any interface.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Example To configure a route of 2001:DB8:1::/48 on eth1.1, with a lifetime of 6000 seconds and a high preference, use the commands:

```
awplus# configure terminal
awplus(config)# int eth1.1
awplus(config-if)# ipv6 nd route-information 2001:DB8:1::/48
6000 high
```

Related commands ipv6 nd suppress-ra

Command changes Version 5.5.0-2.4: command added

ipv6 nd router-preference

Overview Use this command to set the default router preference in the router advertisements sent on a particular interface. You can use this setting to decide whether devices will use this router instead of an alternative router, by giving this router and the alternative router different values.

Use the **no** variant of this command to return the router preference to its default value.

Syntax

```
ipv6 nd router-preference {low|medium|high}
no ipv6 nd router-preference
```

Parameter	Description
`low`	(0b11) Preference for this router on this interface is low.
`medium`	(0b00) Preference for this router on this interface is medium.
`high`	(0b01) Preference for this router on this interface is high.

Default Medium

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Example To set the router preference to high on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 nd router-preference high
```

Related commands ipv6 nd suppress-ra

show ipv6 interface

Command changes Version 5.5.1-0.1: command added

ipv6 nd suppress-ra

Overview Use this command to inhibit IPv6 Router Advertisement (RA) transmission for the current interface. Router advertisements are used when applying IPv6 stateless auto-configuration.

Use the **no** parameter with this command to enable Router Advertisement transmission.

Syntax

```
ipv6 nd suppress-ra
no ipv6 nd suppress-ra
```

Default Router Advertisement (RA) transmission is suppressed by default.

Mode Interface Configuration for an Eth interface, an 802.1Q sub-interface, a local loopback interface, a bridge, or a tunnel.

Example To enable the transmission of router advertisements from eth0 on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 nd suppress-ra
```

Related commands

ipv6 nd ra-interval

ipv6 nd router-preference

ipv6 nd prefix

ipv6 opportunistic-nd

Overview Use this command to enable opportunistic neighbor discovery for the global IPv6 ND cache. Opportunistic neighbor discovery changes the behavior for unsolicited ICMPv6 ND packet forwarding on the device.

Use the **no** variant of this command to disable opportunistic neighbor discovery for the global IPv6 ND cache.

Syntax

```
ipv6 opportunistic-nd
no ipv6 opportunistic-nd
```

Default Opportunistic neighbor discovery is disabled by default.

Mode Global Configuration

Usage notes When opportunistic neighbor discovery is enabled, the device will reply to any received unsolicited ICMPv6 ND packets. The source MAC address for the unsolicited ICMPv6 ND packet is added to the IPv6 ND cache, so the device forwards the ICMPv6 ND packet. When opportunistic neighbor discovery is disabled, the source MAC address for the ICMPv6 packet is not added to the IPv6 ND cache, so the ICMPv6 ND packet is not forwarded by the device.

Examples To enable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# ipv6 opportunistic-nd
```

To disable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# no ipv6 opportunistic-nd
```

Related commands

arp opportunistic-nd

show ipv6 neighbors

show running-config interface

ipv6 route

Overview This command adds a static IPv6 route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to forward packets and to advertise routes to neighbors.

The **no** variant of this command removes the static route.

Syntax

```
ipv6 route <dest-prefix/length> {<gateway-ip>|<gateway-name>}
[<src-prefix/length>] [<distvalue>] [description
<description>]
```

```
no ipv6 route <dest-prefix/length>
{<gateway-ip>|<gateway-name>} [<src-prefix/length>]
[<distvalue>]
```

Parameter	Description
<dest-prefix/length>	Specifies the destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<gateway-ip>	Specifies the address of the gateway (or next hop). The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<gateway-name>	Specifies the name of the interface for the gateway (or next hop).
<src-prefix/length>	Specifies the source prefix. This is used for SADR - see the Usage notes. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<distvalue>	Specifies the administrative distance for the route. Valid values are from 1 to 255. You can use administrative distance to determine which routes take priority over other routes. The route with the lowest distance value is used.
description *<description>*	A description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command **show running-configuration**.

Mode Global Configuration

Usage notes You can configure IPv6 static routes for Source Address Dependent Routing (SADR) by providing a source prefix. In 'normal' routing, when the device searches

routes for a next hop to forward a packet to, the device chooses the next hop based only on the destination address of the packet. When you provide SADR information for a route, the device also inspects the source address and ensures it fits within the source prefix range you provided for this route.

Versions of AlliedWare Plus earlier than 5.5.1-2.1 do not support descriptions on static routes, so a start-up configuration that contains descriptions will be rejected by these older versions. If you add descriptions, be careful if you downgrade to an older AlliedWare Plus version.

Example To create a route with administrative distance of 32 to send packets to 2001:0db8::1/128 via eth1.1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 32
```

To use SADR to create a route for packets from 2001::/64 to 2223::/64, with a next hop of 2001::1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2223::/64 2001::1 2001::/64
```

To give a route a description of 'test' when creating it, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 description
test
```

To remove the description from a route, re-enter the route without specifying the **description** parameter:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1
```

Related Commands show running-config

show ipv6 route

Command changes Version 5.5.1-2.1: **description** parameter added

Version 5.5.0-0.3: **src-prefix** parameter added

ipv6 unreachables

Overview Use this command to enable ICMPv6 (Internet Control Message Protocol version 6) type 1, destination unreachable, messages.

Use the **no** variant of this command to disable destination unreachable messages. This prevents an attacker from using these messages to discover the topology of a network.

Syntax

```
ipv6 unreachables
no ipv6 unreachables
```

Default Destination unreachable messages are enabled by default.

Mode Global Configuration

Usage notes When a device receives a packet for a destination that is unreachable it returns an ICMPv6 type 1 message. This message includes a reason code, as per the table below. An attacker can use these messages to obtain information regarding the topology of a network. Disabling destination unreachable messages, using the **no ipv6 unreachables** command, secures your network against this type of probing.

NOTE: *Disabling ICMPv6 destination unreachable messages breaks applications such as traceroute, which depend on these messages to operate correctly.*

Table 14-1: ICMPv6 type 1 reason codes and description

Code	Description [RFC]
0	No route to destination [RFC4443]
1	Communication with destination administratively prohibited [RFC4443]
2	Beyond scope of source address [RFC4443]
3	Address unreachable [RF4443]
4	Port unreachable [RFC4443]
5	Source address failed ingress/egress policy [RFC4443]
6	Reject route to destination [RFC4443
7	Error in Source Routing Header [RFC6554]

Example To disable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# no ipv6 unreachables
```

To enable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# ipv6 unreachables
```

ping ipv6

Overview This command sends a query to another IPv6 host (send Echo Request messages).

Syntax

```
ping ipv6 {<host>|<ipv6-address>} [repeat
{<1-2147483647>|continuous}] [size <10-1452>] [interface
<interface-list>] [timeout <1-65535>]
```

Parameter	Description
<ipv6-addr>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<hostname>	The destination hostname.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
size *<10-1452>*	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
interface *<interface-list>*	The interface or range of configured IP interfaces to use as the source in the IP header of the ping packet. The interface can be one of: • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the **encapsulation dot1q** command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. You can only specify the interface when pinging a link local address.
timeout *<1-65535>*	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
continuous	Continuous ping.
size *<10-1452>*	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
timeout *<1-65535>*	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.

Mode User Exec and Privileged Exec

Example
```
awplus# ping ipv6 2001:0db8::a2
```

Related commands traceroute ipv6

show ipv6 forwarding

Overview Use this command to display IPv6 forwarding status.

Syntax

```
show ipv6 forwarding
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 forwarding
```

Output Figure 14-1: Example output from the **show ipv6 forwarding** command

```
awplus#show ipv6 forwarding
ipv6 forwarding is on
```

show ipv6 interface

Overview Use this command to display brief information about interfaces and the IPv6 address assigned to them.

Syntax

```
show ipv6 interface [brief|<interface-list>] [nd]
```

Parameter	Description
`brief`	Specify this optional parameter to display brief IPv6 interface information.
<interface-list>	The interfaces to display information about. An interface-list can be: • an Eth interface (e.g. eth0) • an 802.1Q Ethernet sub-interface (e.g. eth0.10, where '10' is the VLAN ID specified by the **encapsulation dot1q** command). Ranges of sub-interfaces are not supported. • a bridge interface (e.g. br0) • the loopback interface (lo) • a continuous range of interfaces, separated by a hyphen (e.g. eth0-eth4) • a comma-separated list (e.g. eth0,eth2-eth4). Do not mix interface types in a list. The specified interfaces must exist.
`nd`	Specify this optional parameter for Neighbor Discovery configurations.

Mode User Exec and Privileged Exec

Examples To display a brief list of all interfaces on a device, use the following command:

```
awplus# show ipv6 interface brief
```

Output Figure 14-2: Example output from the **show ipv6 interface brief** command

```
awplus#show ipv6 interface brief
Interface     IPv6-Address                                Status      Protocol
eth1          unassigned                                  admin up    running
eth1.1        2001:db8::1/48                              admin up    down
              fe80::215:77ff:fee9:5c50/64
lo            unassigned                                  admin up    running
```

Related commands ipv6 nd router-preference

show interface brief

show ipv6 neighbors

Overview Use this command to display all IPv6 neighbors.

For information on filtering and saving command output, see the "Getting_Started with AlliedWare Plus" Feature Overview and Configuration_Guide.

Syntax

```
show ipv6 neighbors
```

Mode User Exec and Privileged Exec

Example To display a device's IPv6 neighbors, use the following command:

```
awplus# show ipv6 neighbors
```

Output Figure 14-3: Example output of the **show ipv6 neighbors** command

```
IPv6 Address                    MAC Address    Interface          Port      Type
fe80::34a9:55ff:fed4:588        36a9.55d4.0588 vlink13 (ATMF)     -         dynamic
```

Related commands clear ipv6 neighbors

show ipv6 route

Overview Use this command to display the IPv6 routing table for a protocol or from a particular table.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 route
[connected|database|static|summary|<ipv6-address>|
<ipv6-prefix/prefix-length>]
```

Parameter	Description
`connected`	Displays only the routes learned from connected interfaces.
`database`	Displays only the IPv6 routing information extracted from the database.
`static`	Displays only the IPv6 static routes you have configured.
`summary`	Displays summary information from the IPv6 routing table.
`<ipv6-address>`	Displays the routes for the specified address in the IPv6 routing table.
`<ipv6-prefix>/<prefix-length>`	Displays only the routes for the specified IPv6 prefix.

Mode User Exec and Privileged Exec

Example To display all IPv6 routes with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

To display all database entries for all IPv6 routes, use the following command:

```
awplus# show ipv6 route database
```

Output Figure 14-4: Example output of the **show ipv6 route** command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
S   ::/0 [1/0] via 2001::a:0:0:c0a8:a6, eth1
C   2001:db8::a:0:0:0:0/64 via ::, eth1
...
```

Output Figure 14-5: Example output of the **show ipv6 route database** command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
> - selected route, * - FIB route, p - stale info
Timers: Uptime

S   ::/0 [1/0] via 2001::a:0:0:c0a8:a01 inactive, 6d22h12m
         [1/0] via 2001::fa:0:0:c0a8:fa01 inactive, 6d22h12m
```

show ipv6 route summary

Overview Use this command to display the summary of the current NSM RIB entries.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 route summary
```

Mode User Exec and Privileged Exec

Example To display IP route summary, use the following command:

```
awplus# show ipv6 route summary
```

Output Figure 14-6: Example output from the **show ipv6 route summary** command

```
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 4
RouteSource     Networks
connected       4
rip             5
Total           9
FIB             5
```

Related commands show ip route database

traceroute ipv6

Overview Use this command to trace the route to the specified IPv6 host.

Syntax

```
traceroute ipv6 {<ipv6-addr>|<hostname>}
```

Parameter	Description
<ipv6-addr>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<hostname>	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

15 Routing Commands

Introduction

Overview This chapter provides an alphabetical reference of routing commands that are common across the routing IP protocols. For more information, see the Route Selection Feature Overview and Configuration Guide.

Command List

- "ip route" on page 404
- "ipv6 route" on page 406
- "show ip route" on page 408
- "show ip route database" on page 410
- "show ip route summary" on page 411
- "show ipv6 route" on page 412
- "show ipv6 route summary" on page 414

ip route

Overview This command adds a static route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to advertise routes to neighbors and forward packets.

The **no** variant of this command removes the static route from the RIB and FIB.

Syntax

```
ip route <subnet&mask> {<gateway-ip>|<interface>} [<distance>]
[description <description>]
```

```
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 interface that connects your device to the network. The gateway IP address or the interface is required.
<distance>	The administrative distance for the static route in the range 1 to 255. Static routes by default have an administrative distance of 1, which gives them the highest priority possible.
description *<description>*	A description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command **show running-configuration**.

Mode Global Configuration

Default The default administrative distance for a static route is 1.

Usage notes You can use administrative distance to determine which routes take priority over other routes.

Versions of AlliedWare Plus earlier than 5.5.1-2.1 do not support descriptions on static routes, so a start-up configuration that contains descriptions will be rejected by these older versions. If you add descriptions, be careful if you downgrade to an older AlliedWare Plus version.

Examples

To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at 10.10.0.2 with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To remove the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at 10.10.0.2 with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# no ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at 10.10.0.2 with an administrative distance of 128, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
128
```

To give a route a description of 'test' when creating it, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0/24 10.10.0.2 description
test
```

To remove the description from a route, re-enter the route without specifying the **description** parameter:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0/24 10.10.0.2
```

Related commands

show ip route

show ip route database

ipv6 route

Overview This command adds a static IPv6 route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to forward packets and to advertise routes to neighbors.

The **no** variant of this command removes the static route.

Syntax

```
ipv6 route <dest-prefix/length> {<gateway-ip>|<gateway-name>}
[<src-prefix/length>] [<distvalue>] [description
<description>]
```

```
no ipv6 route <dest-prefix/length>
{<gateway-ip>|<gateway-name>} [<src-prefix/length>]
[<distvalue>]
```

Parameter	Description
<dest-prefix/length>	Specifies the destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<gateway-ip>	Specifies the address of the gateway (or next hop). The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<gateway-name>	Specifies the name of the interface for the gateway (or next hop).
<src-prefix/length>	Specifies the source prefix. This is used for SADR - see the Usage notes. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<distvalue>	Specifies the administrative distance for the route. Valid values are from 1 to 255. You can use administrative distance to determine which routes take priority over other routes. The route with the lowest distance value is used.
description *<description>*	A description to record the route's purpose. It can be up to 80 printable ASCII characters long, including spaces. The description does not affect routing or forwarding decisions made by the device. To see the description, use the command **show running-configuration**.

Mode Global Configuration

Usage notes You can configure IPv6 static routes for Source Address Dependent Routing (SADR) by providing a source prefix. In 'normal' routing, when the device searches

routes for a next hop to forward a packet to, the device chooses the next hop based only on the destination address of the packet. When you provide SADR information for a route, the device also inspects the source address and ensures it fits within the source prefix range you provided for this route.

Versions of AlliedWare Plus earlier than 5.5.1-2.1 do not support descriptions on static routes, so a start-up configuration that contains descriptions will be rejected by these older versions. If you add descriptions, be careful if you downgrade to an older AlliedWare Plus version.

Example To create a route with administrative distance of 32 to send packets to 2001:0db8::1/128 via eth1.1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 32
```

To use SADR to create a route for packets from 2001::/64 to 2223::/64, with a next hop of 2001::1, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2223::/64 2001::1 2001::/64
```

To give a route a description of 'test' when creating it, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1 description
test
```

To remove the description from a route, re-enter the route without specifying the **description** parameter:

```
awplus# configure terminal
awplus(config)# ipv6 route 2001:0db8::1/128 eth1.1
```

Related Commands show running-config

show ipv6 route

Command changes Version 5.5.1-2.1: **description** parameter added

Version 5.5.0-0.3: **src-prefix** parameter added

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

Examples 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 15-1: Example output from the **show ip route** command

```
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default

Gateway of last resort is 10.34.180.254 to network 0.0.0.0

S*      0.0.0.0/0 [1/0] via 10.34.180.254, eth0.1034
C       10.34.0.0/16 is directly connected, eth0.1034
C       10.10.31.0/24 is directly connected, eth0.2
C       192.168.3.0/24 is directly connected, eth0.3
```

Connected Route An example of a connected route entry consists of:

```
C       10.10.31.0/24 is directly connected, eth0.2
```

This route entry denotes:

- Route entries for network 10.10.31.0/24 are derived from the IP address of local interface eth0.2.
- These routes are marked as Connected routes (C) and always preferred over routes for the same network learned from other routing protocols.

Related commands

ip route

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 15-2: Example output from the **show ip route database** command:

```
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
              > - selected route, * - FIB route, p - stale info

S     *> 0.0.0.0/0 [1/0] via 10.34.180.254, eth0.1034
C     *> 10.34.0.0/16 is directly connected, eth0.1034
C     *> 192.168.2.0/24 is directly connected, eth0.2
C     *> 192.168.3.0/24 is directly connected, eth0.3

Gateway of last resort is not set
```

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 15-3: 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           5
```

Related commands

show ip route

show ip route database

show ipv6 route

Overview Use this command to display the IPv6 routing table for a protocol or from a particular table.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 route
[connected|database|static|summary|<ipv6-address>|
<ipv6-prefix/prefix-length>]
```

Parameter	Description
`connected`	Displays only the routes learned from connected interfaces.
`database`	Displays only the IPv6 routing information extracted from the database.
`static`	Displays only the IPv6 static routes you have configured.
`summary`	Displays summary information from the IPv6 routing table.
`<ipv6-address>`	Displays the routes for the specified address in the IPv6 routing table.
`<ipv6-prefix>/<prefix-length>`	Displays only the routes for the specified IPv6 prefix.

Mode User Exec and Privileged Exec

Example To display all IPv6 routes with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

To display all database entries for all IPv6 routes, use the following command:

```
awplus# show ipv6 route database
```

Output Figure 15-4: Example output of the **show ipv6 route** command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
S   ::/0 [1/0] via 2001::a:0:0:c0a8:a6, eth1
C   2001:db8::a:0:0:0:0/64 via ::, eth1
...
```

Output Figure 15-5: Example output of the **show ipv6 route database** command

```
IPv6 Routing Table
Codes: C - connected, S - static, R - RIP, O - OSPF, B - BGP
> - selected route, * - FIB route, p - stale info
Timers: Uptime

S   ::/0 [1/0] via 2001::a:0:0:c0a8:a01 inactive, 6d22h12m
         [1/0] via 2001::fa:0:0:c0a8:fa01 inactive, 6d22h12m
```

show ipv6 route summary

Overview Use this command to display the summary of the current NSM RIB entries.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 route summary
```

Mode User Exec and Privileged Exec

Example To display IP route summary, use the following command:

```
awplus# show ipv6 route summary
```

Output Figure 15-6: Example output from the **show ipv6 route summary** command

```
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 4
RouteSource     Networks
connected       4
rip             5
Total           9
FIB             5
```

Related commands show ip route database

Part 4: Access and Security

16 AAA Commands

Introduction

Overview

AAA is the collective title for the three related functions of Authentication, Authorization and Accounting. These functions can be applied in a variety of methods with a variety of servers.

The purpose of the AAA commands is to map instances of the AAA functions to sets of servers. The Authentication function can be performed in multiple contexts, such as authentication of users logging in at a console, or 802.1X-Authentication of devices connecting to Ethernet ports.

For each of these contexts, you may want to use different sets of servers for examining the proffered authentication credentials and deciding if they are valid. AAA Authentication commands enable you to specify which servers will be used for different types of authentication.

This chapter provides an alphabetical reference for AAA commands for Authentication, Authorization and Accounting. For more information, see the AAA and Port_Authentication Feature Overview and Configuration Guide.

Command List

- "aaa accounting commands" on page 418
- "aaa accounting login" on page 420
- "aaa authentication download-portal" on page 423
- "aaa authentication enable default group tacacs+" on page 425
- "aaa authentication enable default local" on page 427
- "aaa authentication login" on page 428
- "aaa authorization commands" on page 431
- "aaa authorization config-commands" on page 433
- "aaa group server" on page 434
- "aaa local authentication attempts lockout-time" on page 436
- "aaa local authentication attempts max-fail" on page 437

- "aaa local authentication attempts max-fail remote-login-only" on page 438
- "aaa login fail-delay" on page 439
- "accounting login" on page 440
- "authorization commands" on page 441
- "clear aaa local user lockout" on page 443
- "debug aaa" on page 444
- "login authentication" on page 445
- "proxy-port" on page 446
- "radius-secure-proxy aaa" on page 447
- "server (radsecproxy-aaa)" on page 448
- "server mutual-authentication" on page 450
- "server name-check" on page 451
- "server trustpoint" on page 452
- "show aaa local user locked" on page 454
- "show aaa server group" on page 456
- "show debugging aaa" on page 457
- "show radius server group" on page 458
- "undebug aaa" on page 460

aaa accounting commands

Overview This command configures and enables TACACS+ accounting on commands entered at a specified privilege level. Once enabled for a privilege level, accounting messages for commands entered at that privilege level will be sent to a TACACS+ server.

In order to account for all commands entered on a device, configure command accounting for each privilege level separately.

The command accounting message includes, the command as entered, the date and time the command finished executing, and the user-name of the user who executed the command.

Use the **no** variant of this command to disable command accounting for a specified privilege level.

Syntax

```
aaa accounting commands <1-15> default stop-only group tacacs+
no aaa accounting commands <1-15> default
```

Parameter	Description
<1-15>	The privilege level being configured, in the range 1 to 15.
`default`	Use the default method list, this means the command is applied globally to all user exec sessions.
`stop-only`	Send accounting message when the commands have stopped executing.
`group`	Specify the server group where accounting messages are sent. Only the tacacs+ group is available for this command.
`tacacs+`	Use all TACACS+ servers configured by the tacacs-server host command.

Default TACACS+ command accounting is disabled by default.

Mode Global Configuration

Usage notes This command only supports a **default** method list, this means that it is applied to every console and VTY line.

The **stop-only** parameter indicates that the command accounting messages are sent to the TACACS+ server when the commands have stopped executing.

The **group tacacs+** parameters signifies that the command accounting messages are sent to the TACACS+ servers configured by the tacacs-server host command.

Note that up to four TACACS+ servers can be configured for accounting. The servers are checked for reachability in the order they are configured with only the first reachable server being used. If no server is found, the accounting message is dropped.

Command accounting cannot coexist with triggers. An error message is displayed if you attempt to enable command accounting while a trigger is configured. Likewise, an error message is displayed if you attempt to configure a trigger while command accounting is configured.

Examples

To configure command accounting for privilege levels 1, 7, and 15, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting commands 1 default stop-only
group tacacs+
awplus(config)# aaa accounting commands 7 default stop-only
group tacacs+
awplus(config)# aaa accounting commands 15 default stop-only
group tacacs+
```

To disable command accounting for privilege levels 1, 7, and 15, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting commands 1 default
awplus(config)# no aaa accounting commands 7 default
awplus(config)# no aaa accounting commands 15 default
```

Related commands

aaa authentication login

aaa accounting login

accounting login

tacacs-server host

aaa accounting login

Overview This command configures RADIUS and TACACS+ accounting for login shell sessions. The specified method list name can be used by the **accounting login** command in the Line Configuration mode. If the **default** parameter is specified, then this creates a default method list that is applied to every console and VTY line, unless another accounting method list is applied on that line.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to remove an accounting method list for login shell sessions configured by an **aaa accounting login** command. If the method list being deleted is already applied to a console or VTY line, accounting on that line will be disabled. If the default method list name is removed by this command, it will disable accounting on every line that has the default accounting configuration.

Syntax

```
aaa accounting login
{default|<list-name>}{start-stop|stop-only|none} {group
{radius|tacacs+|<group-name>}}
```

```
no aaa accounting login {default|<list-name>}
```

Parameter	Description
`default`	Default accounting method list.
`<list-name>`	Named accounting method list.
`start-stop`	Start and stop records to be sent.
`stop-only`	Stop records to be sent.
`none`	No accounting record to be sent.
`group`	Specify the servers or server group where accounting packets are sent.
`radius`	Use all RADIUS servers configured by the radius-server host command.
`tacacs+`	Use all TACACS+ servers configured by the tacacs-server host command.
`<group-name>`	Use the specified RADIUS server group, as configured by the aaa group server command.

Default Accounting for login shell sessions is disabled by default.

Mode Global Configuration

Usage notes

This command enables you to define a named accounting method list. The items that you define in the accounting options are:

- the types of accounting packets that will be sent
- the set of servers to which the accounting packets will be sent

You can define a default method list with the name **default** and any number of other named method lists. The name of any method list that you define can then be used as the *<list-name>* parameter in the accounting login command.

If the method list name already exists, the command will replace the existing configuration with the new one.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by radius-server host command
- **group** *<group-name>* : use the specified RADIUS server group configured with the aaa group server command

There is one way to define servers where TACACS+ accounting messages are sent:

- **group tacacs+** : use all TACACS+ servers configured by tacacs-server host command

The accounting event to send to the RADIUS or TACACS+ server is configured with the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Examples

To configure RADIUS accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group radius
```

To configure TACACS+ accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group tacacs+
```

To reset the configuration of the default accounting list, use the following commands:

```
awplus# configure terminal
awplus(config)#  no aaa accounting login default
```

Related commands

aaa accounting commands

aaa authentication login

aaa accounting login

accounting login

radius-server host

tacacs-server host

aaa authentication download-portal

Overview Use this command to globally enable authentication, and set the default authentication method, for Download Portal clients. The default authentication method can be:

- all configured RADIUS servers,
- all configured LDAP servers,
- or a user-defined group of RADIUS or LDAP servers.

Use the **no** variant of this command to globally disable authentication on for Download Portal Clients.

Syntax

```
aaa authentication download-portal default group
[<group-name>|radius|ldap]
```

```
no aaa authentication download-portal default
```

Parameter	Description
<group-name>	Server group name.
radius	Use all RADIUS servers
ldap	Use all LDAP servers

Default Authentication for Download Portal clients is disabled by default.

Mode Global Configuration

Usage notes There are a number of ways to define groups of authentication servers. These are:

- **group radius**: use all RADIUS servers configured with the radius-server host command.
- **group ldap**: use all LDAP servers configured with the ldap-server command.
- **group <group-name>**: use the specified RADIUS or LDAP server group configured with the aaa group server command.

Example To enable LDAP authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authentication download-portal default
group ldap
```

To use a server group to authenticate Download Portal clients, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authentication download-portal default
group my_group
```

Note: This could be a group of RADIUS or LDAP servers.

To disable authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication download-portal default
```

Related commands

aaa group server

download-portal

Command changes

Version 5.5.4-0: command added

aaa authentication enable default group tacacs+

Overview This command enables privilege level authentication against a TACACS+ server.

Use the **no** variant of this command to disable privilege level authentication.

Syntax

```
aaa authentication enable default group tacacs+ [local] [none]
no aaa authentication enable default
```

Parameter	Description
`local`	Use the locally configured enable password (**enable password** command) for authentication.
`none`	No authentication.

Default Local privilege level authentication is enabled by default (aaa authentication enable default local command).

Mode Global Configuration

Usage notes A user is configured on a TACACS+ server with a maximum privilege level. When they enter the enable (Privileged Exec mode) command they are prompted for an enable password which is authenticated against the TACACS+ server. If the password is correct and the specified privilege level is equal to or less than the users maximum privilege level, then they are granted access to that level. If the user attempts to access a privilege level that is higher than their maximum configured privilege level, then the authentication session will fail and they will remain at their current privilege level.

NOTE: *If both **local** and **none** are specified, you must always specify **local** first.*

If the TACACS+ server goes offline, or is not reachable during enable password authentication, and command level authentication is configured as:

- **aaa authentication enable default group tacacs+**

  then the user is never granted access to Privileged Exec mode.

- **aaa authentication enable default group tacacs+ local**

  then the user is authenticated using the locally configured enable password, which if entered correctly grants the user access to Privileged Exec mode. If no enable password is locally configured (**enable password** command), then the enable authentication will fail until the TACACS+ server becomes available again.

- **aaa authentication enable default group tacacs+ none**

  then the user is granted access to Privileged Exec mode with no authentication. This is true even if a locally configured enable password is configured.

- **aaa authentication enable default group tacacs+ local none**

  then the user is authenticated using the locally configured enable password. If no enable password is locally configured, then the enable authentication will grant access to Privileged Exec mode with no authentication.

If the password for the user is not successfully authenticated by the server, then the user is again prompted for an enable password when they enter **enable** via the CLI.

Examples

To enable a privilege level authentication method that will not allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default group tacacs+
```

To enable a privilege level authentication method that will allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, and a locally configured enable password is configured, use the following commands:

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

To disable privilege level authentication, use the following commands:

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

Related commands

aaa authentication login

aaa authentication enable default local

enable (Privileged Exec mode)

enable password

enable secret (deprecated)

tacacs-server host

aaa authentication enable default local

Overview This command enables local privilege level authentication.

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

Syntax

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

Default Local privilege level authentication is enabled by default.

Mode Global Configuration

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

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

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

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

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

Related commands

aaa authentication login

enable (Privileged Exec mode)

enable password

enable secret (deprecated)

aaa authentication login

Overview Use this command to create an ordered list of methods for authenticating user logins. It can also be used to replace an existing method list with a list of the same name. Specify one or more of the options **local** or **group**, in the order you want them to be applied. If the **default** method list name is specified, it is applied to every console and VTY line immediately unless another method list is applied to that line by the login authentication command. To apply a non-default method list, you must also use the login authentication command.

Use the **no** variant of this command to remove a method list from user login authentication. The specified method list name is deleted from the configuration. If the method list name has been applied to any console or VTY line, user login authentication on that line will fail.

Note that the **no aaa authentication login default** command does not remove the default method list. This will return the default method list to its default state (**local** is the default).

Syntax

```
aaa authentication login {default|<list-name>} {[local] [group
{radius|ldap|tacacs+|<group-name>}]}
```

```
no aaa authentication login {default|<list-name>}
```

Parameter	Description
`default`	Set the default authentication server for user login.
`<list-name>`	Name of authentication server.
`local`	Use the local username database.
`group`	Use server group.
`radius`	Use all RADIUS servers configured by the radius-server host command.
`ldap`	Use all LDAP servers configured by the ldap-server command.
`tacacs+`	Use all TACACS+ servers configured by the tacacs-server host command.
`<group-name>`	Use the specified RADIUS or LDAP server group.

Default If the default server is not configured using this command, user login authentication uses the local user database only.

If the **default** method list name is specified, it is applied to every console and VTY line immediately unless a named method list server is applied to that line by the **login authentication** command.

local is the default state for the default method list unless a named method list is applied to that line by the **login authentication** command. You can reset it to the default method list using the **no aaa authentication login default** command.

Mode Global Configuration

Usage notes When a user attempts to log in, the switch sends an authentication request to the first authentication server in the method list. If the first server in the list is reachable and it contains a username and password matching the authentication request, the user is authenticated and the login succeeds. If the authentication server denies the authentication request because of an incorrect username or password, the user login fails. If the first server in the method list is unreachable, the switch sends the request to the next server in the list, and so on.

For example, if the method list specifies **group tacacs+ local**, and a user attempts to log in with a password that does not match a user entry in the first TACACS+ server, if this TACACS+ server denies the authentication request, then the switch does not try any other TACACS+ servers nor the local user database; the user login fails.

Examples To configure the default authentication method list for user login to first use all available RADIUS servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login default group radius
local
```

To configure the default authentication method list for user login to first use all available LDAP servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login default group ldap
local
```

To configure a user login authentication method list called 'USERS' to first use the RADIUS server group 'RAD_GROUP1' for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group RAD_GROUP1
local
```

To configure a user login authentication method list called 'USERS' to first use the TACACS+ servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group tacacs+
local
```

To return to the default method list (**local** is the default server), use the following commands:

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

To delete an existing authentication method list 'USERS' created for user login authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication login USERS
```

Related commands

aaa accounting commands

aaa authentication enable default group tacacs+

ldap-server

login authentication

radius-server host

Command changes

Version 5.5.2-1.1: **ldap** parameter added

aaa authorization commands

Overview This command configures a method list for commands authorization that can be applied to console or VTY lines. When command authorization is enabled for a privilege level, only authorized users can executed commands in that privilege level.

Use the **no** variant of this command to remove a named method list or disable the default method list for a privilege level.

Syntax

```
aaa authorization commands <privilege-level>
{default|<list-name>} group tacacs+ [none]
```

```
no aaa authorization commands <privilege-level>
{default|<list-name>}
```

Parameter	Description
<privilege-level>	The privilege level of the set of commands the method list will be applied to. AlliedWare Plus defines three sets of commands, that are indexed by a level value: **Level = 1**: All commands that can be accessed by a user with privilege level between 1 and 6 inclusive **Level = 7:** All commands that can be accessed by a user with privilege level between 7 and 14 inclusive **Level = 15**: All commands that can be accessed by a user with privilege level 15
`group`	Specify the server group where authorization messages are sent. Only the `tacacs+` group is available for this command.
`tacacs+`	Use all TACACS+ servers configured by the tacacs-server host command.
`default`	Configure the default authorization commands method list.
<list-name>	Configure a named authorization commands method list
`none`	If specified, this provides a local fallback to command authorization so that if authorization servers become unavailable then the device will accept all commands normally allowed for the privilege level of the user.

Mode Global Configuration

Usage notes TACACS+ command authorization provides centralized control of the commands available to a user of an AlliedWare Plus device. Once enabled:

- The command string and username are encrypted and sent to the first available configured TACACS+ server (the first server configured) for authorization.

- The TACACS+ server decides if the user is authorized to execute the command and returns the decision to the AlliedWare Plus device.
- Depending on this decision the device will then either execute the command or notify the user that authorization has failed.

If multiple TACACS+ servers are configured, and the first server is unreachable or does not respond, the other servers will be queried, in turn, for an authorization decision. If all servers are unreachable and a local fallback has been configured, with the **none** parameter, then commands are authorized based on the user's privilege level; the same behavior as if command authorization had not been configured. If, however, the local fallback is not configured and all servers become unreachable then all commands except **logout**, **exit**, and **quit** will be denied.

The **default** method list is defined with a local fallback unless configured differently using this command.

Example To configure a commands authorization method list, named TAC15, using all TACACS+ servers to authorize commands for privilege level 15, with a local fallback, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authorization commands 15 TAC15 group tacacs+ none
```

To configure the default method list to authorize commands for privilege level 7, with no local fallback, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authorization commands 7 default group tacacs+
```

To remove the authorization method list TAC15, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authorization commands 15 TAC15
```

Related commands

aaa authorization config-commands

authorization commands

tacacs-server host

Command changes Version 5.4.6-2.1: command added

aaa authorization config-commands

Overview Use this command to enable command authorization on configuration mode commands. By default, command authorization applies to commands in exec mode only.

Use the **no** variant of this command to disable command authorization on configuration mode commands.

Syntax

```
aaa authorization config-commands
no aaa authorization config-commands
```

Default By default, command authorization is disabled on configuration mode commands.

Mode Global Configuration

Usage notes If authorization of configuration mode commands is not enabled then all configuration commands are accepted by default, including command authorization commands.

NOTE: *Authorization of configuration commands is required for a secure TACACS+ command authorization configuration as it prevents the feature from being disabled to gain access to unauthorized exec mode commands.*

Example To enable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authorization config-commands
```

To disable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authorization config-commands
```

Related commands aaa authorization commands

authorization commands

tacacs-server host

Command changes Version 5.4.6-2.1: command added

aaa group server

Overview Use this command to create an AAA group of RADIUS or LDAP servers, and to enter Server Group Configuration mode.

A server group is used to specify a subset of RADIUS or LDAP servers in AAA commands. Once in Server Group Configuration mode you can add servers to the group.

Use the **no** variant of this command to remove an existing server group.

Syntax

```
aaa group server {radius|ldap} <group-name>
no aaa group server {radius|ldap} <group-name>
```

Parameter	Description
`radius`	Create or configure a RADIUS server group.
`ldap`	Create or configure an LDAP server group.
<group-name>	Server group name.

Mode Global Configuration

Usage notes To add servers to a RADIUS or LDAP server group, use the **server** command. Each RADIUS server in a server group must be configured using the radius-server host command. Similarly, each LDAP server in a server group must be configured using the ldap-server command.

Server groups named 'radius' and 'ldap' are predefined and include all RADIUS and LDAP servers configured using the radius-server host or ldap-server commands.

Examples To create a RADIUS server group named 'GROUP1' with hosts 192.168.1.1, 192.168.2.1 and 192.168.3.1, use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.2.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.3.1 auth-port 1812 acct-port 1813
```

To remove a RADIUS server group named 'GROUP1' from the configuration, use the command:

```
awplus(config)# no aaa group server radius GROUP1
```

To create an LDAP server group named 'GROUP2' with servers named 'SERVER1', 'SERVER2' and 'SERVER3', use the commands:

```
awplus(config)# aaa group server ldap GROUP2
awplus(config-ldap-group)# server SERVER1
awplus(config-ldap-group)# server SERVER2
awplus(config-ldap-group)# server SERVER3
```

To remove an LDAP server group named 'GROUP2' from the configuration, use the command:

```
awplus(config)# no aaa group server ldap GROUP2
```

Related commands

aaa accounting login

aaa authentication login

ldap-server

radius-server host

server (ldap-group)

server (RADIUS server group)

show ldap server group

Command changes

Version 5.5.2-1.1: **ldap** parameter added

aaa local authentication attempts lockout-time

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

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

Syntax

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

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

Mode Global Configuration

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

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

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

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

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

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

Related commands

aaa local authentication attempts max-fail

aaa local authentication attempts max-fail remote-login-only

clear aaa local user lockout

aaa local authentication attempts max-fail

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

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

Syntax

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

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

Mode Global Configuration

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

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

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

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

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

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

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

Related commands

aaa local authentication attempts lockout-time

aaa local authentication attempts max-fail remote-login-only

clear aaa local user lockout

aaa local authentication attempts max-fail remote-login-only

Overview Use this command to configure account lockout to remote logins only. This means that console logins are not subject to lock out when this feature is configured.

This command allow users to login via the physical console port even when the account is locked due to reaching the maximum number of failed login attempts.

Use the **no** variant of this command to prevent users from logging in via the console port when the maximum number of failed login attempts is reached.

Syntax

```
aaa local authentication attempts max-fail remote-login-only
no aaa local authentication attempts max-fail remote-login-only
```

Default Not set. Max-fail lockout applies to all logins.

Mode Global Configuration

Example To configure account lock-out to remote login only, use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts max-fail
remote-login-only
```

To configure account lock-out to apply to all logins, use the commands:

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

Related commands aaa local authentication attempts max-fail

aaa local authentication attempts lockout-time

clear aaa local user lockout

Command changes Version 5.5.4-1.2: command added

aaa login fail-delay

Overview Use this command to configure the minimum time period between failed login attempts. This setting applies to login attempts via the console, SSH and Telnet.

Use the **no** variant of this command to reset the minimum time period to its default value.

Syntax

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

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

Default 1 second

Mode Global configuration

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

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

Related commands

aaa authentication login

aaa local authentication attempts 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 Accounting applied to console or VTY lines for local or remote login. **default** login accounting is applied after issuing the **no accounting login** command. Accounting is disabled with **default**.

Syntax

```
accounting login {default|<list-name>}
no accounting login
```

Parameter	Description
`default`	Default accounting method list.
<list-name>	Named accounting method list.

Default By default login accounting is disabled in the **default** accounting server. No accounting will be performed until accounting is enabled using this command.

Mode Line Configuration

Examples To apply the accounting server `USERS` to all VTY lines, use the following commands:

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

Related commands aaa accounting commands

aaa accounting login

authorization commands

Overview This command applies a command authorization method list, defined using the aaa authorization commands command, to console and VTY lines.

Use the **no** variant of this command to reset the command authorization configuration on the console and VTY lines.

Syntax

```
authorization commands <privilege-level> {default|<list-name>}
no authorization commands <privilege-level>
```

Parameter	Description
<privilege-level>	The privilege level of the set of commands the method list will be applied to. AlliedWare Plus defines three sets of commands, that are indexed by a level value: **Level = 1**: All commands that can be accessed by a user with privilege level between 1 and 6 inclusive **Level = 7:** All commands that can be accessed by a user with privilege level between 7 and 14 inclusive **Level = 15**: All commands that can be accessed by a user with privilege level 15
`default`	Configure the default authorization commands method list.
<list-name>	Configure a named authorization commands method list

Default The **default** method list is applied to each console and VTY line by default.

Mode Line Configuration

Usage notes If the specified method list does not exist users will not be enable to execute any commands in the specified method list on the specified VTY lines.

Example To apply the TAC15 command authorization method list with privilege level 15 to VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# authorization commands 15 TAC15
```

To reset the command authorization configuration with privilege level 15 on VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# no authorization commands 15
```

Related commands aaa authorization commands

aaa authorization config-commands

tacacs-server host

Command changes Version 5.4.6-2.1: command added

clear aaa local user lockout

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

Syntax

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

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

Mode Privileged Exec

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

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

To unlock all user accounts use the following command:

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

Related commands aaa local authentication attempts lockout-time

debug aaa

Overview This command enables AAA debugging.

Use the **no** variant of this command to disable AAA debugging.

Syntax

```
debug aaa [accounting|all|authentication|authorization]
no debug aaa [accounting|all|authentication|authorization]
```

Parameter	Description
`accounting`	Accounting debugging.
`all`	All debugging options are enabled.
`authentication`	Authentication debugging.
`authorization`	Authorization debugging.

Default AAA debugging is disabled by default.

Mode Privileged Exec

Examples To enable authentication debugging for AAA, use the command:

```
awplus# debug aaa authentication
```

To disable authentication debugging for AAA, use the command:

```
awplus# no debug aaa authentication
```

Related commands show debugging aaa

undebug aaa

login authentication

Overview Use this command to apply an AAA server for authenticating user login attempts from a console or remote logins on these console or VTY lines. The authentication method list must be specified by the **aaa authentication login** command. If the method list has not been configured by the **aaa authentication login** command, login authentication will fail on these lines.

Use the **no** variant of this command to reset AAA Authentication configuration to use the default method list for login authentication on these console or VTY lines.

Command Syntax

```
login authentication {default|<list-name>}
no login authentication
```

Parameter	Description
`default`	The default authentication method list. If the default method list has not been configured by the aaa authentication login 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

proxy-port

Overview Use this command to change the local UDP port used for communication between local RADIUS client applications and the RadSecProxy AAA application. Any unused UDP port may be selected. The default port is 1645.

Use the **no** variant of this command to change the UDP port back to the default of 1645.

Syntax

```
proxy-port <port>
no proxy-port
```

Parameter	Description
<port>	UDP Port Number, 1-65536.

Default The default port is 1645.

Mode RadSecProxy AAA Configuration Mode

Usage notes It is not necessary to change the value from the default unless UDP port 1645 is required for another purpose.RADIUS requests received on this port from external devices will be ignored. The port is only used for local (intra-device) communication.

Example To configure change the UDP port to 7001, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# proxy-port 7001
```

Related commands

radius-secure-proxy aaa

server (radsecproxy-aaa)

server name-check

server trustpoint

radius-secure-proxy aaa

Overview Use this command to enter the RadSecProxy AAA (authentication, authorization, and accounting) application configuration mode. This application allows local RADIUS-based clients on system to communicate with remote RadSec servers via a secure (TLS) proxy.

Syntax

```
radius-secure-proxy aaa
```

Mode Global Configuration Mode

Example To change mode from User Exec mode to the RadSecProxy AAA configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)#
```

Related commands

proxy-port

server (radsecproxy-aaa)

server name-check

server trustpoint

server (radsecproxy-aaa)

Overview Use this command to add a server to the RadSecProxy AAA application. Local RADIUS client applications will attempt, via the proxy, to communicate with any RadSec servers that are operational (in addition to any non-TLS RADIUS servers that are configured).

Use the **no** variant of this command to delete a previously-configured server from the RadSecProxy AAA application.

Syntax

```
server {<hostname>|<ip-addr>} [timeout <1-1000>] [name-check
{on|off}]
no server {<hostname>|<ip-addr>}
```

Parameter	Description	
<hostname>	Hostname of RadSec server	
<ip-addr>	Specify the client IPv4 address, in dotted decimal notation (A.B.C.D).	
timeout	Specify the amount of time that the RadSecProxy AAA application should wait for replies from this server. RADIUS server timeout (which defaults to 5 seconds).	
<1-1000>	Time in seconds to wait for a server reply.	
name-check	Specify whether or not to enforce certificate name checking for this client. If the parameter is not specified then the global behavior, which defaults to **on**, is used.	
	on	Enable name checking for this client.
	off	Disable name checking for this client.

Mode RadSecProxy AAA Configuration Mode

Usage notes The server may be specified by its domain name or by its IPv4 address. If a domain name is used, it must be resolvable using a configured DNS name server.

Each server may be configured with a timeout; if not specified, the global timeout value for RADIUS servers will be used. The global timeout may be changed using the **radius-server timeout** command. The default global timeout is 5 seconds.

Each server may be configured to use certificate name-checking; if not specified, the global behavior defined by **server name-check** or **no server name-check** will be used. If name checking is enabled, the Common Name portion of the subject field of the server's X.509 certificate must match the domain name or IP address specified in this command.

Example To add a server 'mynas.local' with a timeout of 3 seconds, and name checking off, use the commands:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# server mynas.local name-check
off
```

Related commands

proxy-port

radius-secure-proxy aaa

server name-check

server trustpoint

server mutual-authentication

Overview This command enables or disables mutual certificate authentication for all RadSecProxy servers. When enabled, the RadSecProxy AAA application will send a local X.509 certificate to the server when establishing a TLS connection.

Use the **no** variant of this command to disable mutual certificate validation causing the RadSecProxy AAA application to not transmit a certificate to the server.

NOTE: *If mutual authentication is disabled on the client (AAA) application but enabled on the server, a connection will not be established.*

Syntax

```
server mutual-authentication
no server mutual-authentication
```

Default Mutual authentication is enabled by default.

Mode RadSecProxy AAA Configuration Mode

Example Disable mutual certificate validation with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# no server
mutual-authentication
```

Related commands

radius-secure-proxy aaa

server name-check

server (radsecproxy-aaa)

Command changes Version 5.4.6-2.1: command added

server name-check

Overview This command sets the global behavior for certificate name-checking for the RadSecProxy AAA application to **on**. This behavior will be used for all servers associated with the application that do not specify a behavior on a per-server basis. If name-checking is enabled, the Common Name portion of the subject field of the client's X.509 certificate must match the domain name or IP address specified in the **server (radsecproxy-aaa)** command.

Use the **no** variant of this command to set the global behavior for certificate name checking to **off**

Syntax

```
server name-check
no server name-check
```

Default Certificate name checking is on by default.

Mode RadSecProxy AAA Configuration Mode

Example Disable certificate name checking globally with the following command:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# no server name-check
```

Related commands

proxy-port

radius-secure-proxy aaa

server (radsecproxy-aaa)

server trustpoint

server trustpoint

Overview This command adds one or more trustpoints to be used with the RadSecProxy AAA application. Multiple trustpoints may be specified, or the command may be executed more than once, to add multiple trustpoints to the application.

The **no** version of this command removes one or more trustpoints from the list of trustpoints associated with the application.

Syntax

```
server trustpoint [<trustpoint-list>]
no server trustpoint [<trustpoint-list>]
```

Parameter	Description
<trustpoint-list>	Specify one or more trustpoints to be added or deleted.

Default By default, no trustpoints are associated with the application.

Mode RadSecProxy AAA Configuration Mode

Usage notes The device certificate associated with first trustpoint added to the application will be transmitted to remote servers. The certificate received from the remote server must have an issuer chain that terminates with the root CA certificate for any of the trustpoints that are associated with the application.

If no trustpoints are specified in the command, the trustpoint list will be unchanged.

If **no server trustpoint** is issued without specifying any trustpoints, then all trustpoints will be disassociated from the application.

Example You can add multiple trustpoints to the RadSecProxy AAA application by executing the command multiple times:

```
awplus# configure terminal
awplus(config)# radius-secure-proxy aaa
awplus(config-radsecproxy-aaa)# server trustpoint example_1
awplus(config-radsecproxy-aaa)# server trustpoint example_2
```

Alternatively, add multiple trustpoints with a single command:

```
awplus(config-radsecproxy-aaa)# server trustpoint example_3
example_4
```

Disassociate all trustpoints from the RadSecProxy AAA application using the command:

```
awplus(config-radsecproxy-aaa)# no server trustpoint
```

Related commands proxy-port

radius-secure-proxy aaa

server (radsecproxy-aaa)

server name-check

show aaa local user locked

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

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

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

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

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

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

In the Valid column:

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

Syntax
```
show aaa local user locked
```

Mode User Exec and Privileged Exec

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

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

Output Figure 16-1: Example output from the **show aaa local user locked** command

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

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

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

Related commands

aaa local authentication attempts lockout-time

aaa local authentication attempts max-fail

clear aaa local user lockout

show aaa server group

Overview Use this command to list AAA users and any method lists applied to them.

Syntax

```
show aaa server group
```

Mode Privileged Exec

Example To show the AAA configuration on a device, use the command:

```
awplus# show aaa server group
```

Output Figure 16-2: Example output from **show aaa server group**

```
awplus#show aaa server group
User          List Name     Method                 Acct-Event
======== ==== ============= ================ ======= ==========
login    auth default       -                local   -
-------- ---- ------------- ---------------- ------- ----------
cmd-1    auth -             -                -       -
-------- ---- ------------- ---------------- ------- ----------
cmd-7    auth -             -                -       -
-------- ---- ------------- ---------------- ------- ----------
cmd-15   auth -             -                -       -
-------- ---- ------------- ---------------- ------- ----------
login    acct -             -                -       -
-------- ---- ------------- ---------------- ------- ----------
isakmp   auth default       radius           group   -
-------- ---- ------------- ---------------- ------- ----------
```

show debugging aaa

Overview Use this command to see what debugging is turned on for AAA (Authentication, Authorization, Accounting).

Syntax

```
show debugging aaa
```

Mode User Exec and Privileged Exec

Example To display the current debugging status of AAA, use the command:

```
awplus# show debug aaa
```

Output Figure 16-3: Example output from the **show debug aaa** command

```
AAA debugging status:
 Authentication debugging is on
 Accounting debugging is off
```

show radius server group

Overview Use this command to show the RADIUS server group configuration.

Syntax

```
show radius server group [<group-name>]
```

Parameter	Description
<group-name>	RADIUS server group name.

Default Command name is set to something by default.

Mode Privileged Exec

Usage Use this command with the *<group-name>* parameter to display information for a specific RADIUS server group, or without the parameter to display information for all RADIUS server groups.

Example To display information for all RADIUS server groups, use the command:

```
awplus# show radius server group
```

To display a information for a RADIUS server group named 'rad_group_list1', use the command:

```
awplus# show radius server group rad_group_list1
```

Output Figure 16-4: Example output from **show radius server group**

```
awplus#show radius server group
RADIUS Group Configuration
  Group Name : radius?
    Server Host/     Auth  Acct  Auth    Acct
    IP Address       Port  Port  Status  Status
    ----------------------------------------
    192.168.1.101    1812  1813  Active  Active
    192.168.1.102    1812  1813  Active  Active

  Group Name : rad_group_list1
    Server Host/     Auth  Acct  Auth    Acct
    IP Address       Port  Port  Status  Status
    ----------------------------------------
    192.168.1.101    1812  1813  Active  Active

  Group Name : rad_group_list2
    Server Host/     Auth  Acct  Auth    Acct
    IP Address       Port  Port  Status  Status
    ----------------------------------------
    192.168.1.102    1812  1813  Active  Active
```

Figure 16-5: Example output from **show radius server group rad_group_list1**

```
awplus#show radius server group rad_group_list1
RADIUS Group Configuration
  Group Name : rad_group_list1
    Server Host/    Auth  Acct  Auth    Acct
    IP Address      Port  Port  Status  Status
    ----------------------------------------
    192.168.1.101   1812  1813  Active  Active
```

Related commands aaa group server

undebug aaa

Overview This command applies the functionality of the **no** debug aaa command.

17 Lightweight Directory Access Protocol (LDAP) Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure Lightweight Directory Access Protocol (LDAP).

LDAP is an authentication protocol that facilitates user access to various IT resources e.g. applications, servers, networking equipment, and file servers.

It can be used to connect to internal networks over OpenVPN. Although both LDAP and RADIUS are interchangeable on AlliedWare Plus devices as an authentication protocol, LDAP is added because of its ability to interact with directory services such as Microsoft's Active Directory (AD).

For more information, see the LDAP Feature Overview and Configuration Guide.

Command List

- "authentication (ldap-server)" on page 463
- "base-dn" on page 465
- "bind authenticate root-dn" on page 466
- "deadtime (ldap-server)" on page 467
- "debug ldap client" on page 468
- "group-attribute" on page 470
- "group-dn" on page 471
- "host (ldap-server)" on page 472
- "ldap-server" on page 474
- "login-attribute" on page 476
- "port (ldap-server)" on page 478
- "retransmit (ldap-server)" on page 479
- "search-filter" on page 480
- "secure cipher (ldap-server)" on page 482

- "secure mode (ldap-server)" on page 484
- "secure trustpoint (ldap-server)" on page 486
- "server (ldap-group)" on page 487
- "show ldap server group" on page 488
- "timeout (ldap-server)" on page 490

authentication (ldap-server)

Overview Use this command to set the authentication method used to authenticate users against the Lightweight Directory Access Protocol (LDAP) server.

Use the **no** variant of this command to reset the authentication method to **search**.

Syntax

```
authentication {search|bind-only}
no authentication
```

Parameter	Description
`search`	The **search** method initially binds to the LDAP server, then searches for the user, then binds to the user using the DN found with the search. The initial bind is either anonymous, or using the user specified with the bind authenticate root-dn command.
`bind-only`	The **bind-only** method attempts to bind to the LDAP server using a predicted DN based on the username, the user attribute (set with the login-attribute command) and the base DN (set with the base-dn command). The format of this user DN is as follows: '<username>=<login-attribute>,<base-dn>'.

Default Search

Mode LDAP Server Configuration

Example To set the authentication method to bind-only for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# authentication bind-only
```

To reset the authentication method to the default (search) for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no authentication
```

Related commands

base-dn

bind authenticate root-dn

ldap-server

login-attribute

search-filter

Command changes Version 5.5.2-1.1: command added

base-dn

Overview Use this command to set the base DN (Distinguished Name) of the LDAP server.

When using 'search' authentication, the base DN is the LDAP server's starting point to search for the user within the directory.

If 'bind-only' authentication is enabled, then the base DN is the suffix of the DN that is used to bind to the user.

Use the **no** variant of this command to remove the configured base DN.

Syntax

```
base-dn <base-dn>
no base-dn
```

Parameter	Description
<base-dn>	The base DN of the LDAP server.

Default Not set

Mode LDAP Server Configuration

Example To set the base DN for the LDAP server called 'Server1' to 'dc=example, dc=com', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# base-dn dc=example,dc=com
```

To clear the base DN for Server1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no base-dn
```

Related commands

authentication (ldap-server)

bind authenticate root-dn

group-attribute

group-dn

ldap-server

login-attribute

search-filter

Command changes Version 5.5.2-1.1: command added

bind authenticate root-dn

Overview Use this command to set the authenticated user to bind to when searching for a user on an LDAP server. Do not set this option if you wish to use anonymous binding with the 'search' method.

This option is ignored with the 'bind-only' authentication method.

Use the **no** variant of this command to unset the authenticated user.

Syntax

```
bind authenticate root-dn <user-dn> password <password>
no bind authenticate root-dn
```

Parameter	Description
<user-dn>	The DN of the authenticated user to bind to.
<password>	The password of the authenticated user.

Default Not set

Mode LDAP Server Configuration

Example To set the authenticated user to 'cn=admin,dc=example,dc=com' with the password '12345678' for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# bind authenticate root-dn
cn=admin,dc=example,dc=com password 12345678
```

Related commands

authentication (ldap-server)

base-dn

group-attribute

ldap-server

login-attribute

search-filter

Command changes Version 5.5.2-1.1: command added

deadtime (ldap-server)

Overview Use this command to configure the deadtime for an LDAP server. The configured deadtime is how long in seconds before an unresponsive LDAP server is considered dead.

Use the **no** variant of this command to remove the deadtime configured on an LDAP server. When you remove the deadtime, the server will never be considered dead.

Syntax

```
deadtime <0-1440>
no deadtime
```

Parameter	Description
<0-1440>	The number of seconds that the server can be unresponsive for before it is considered dead.

Default 0 seconds (the LDAP server is never considered dead)

Mode LDAP Server Configuration

Example To set the deadtime to 20 seconds for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# deadtime 20
```

To reset the deadtime to the default for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no deadtime
```

Related commands

host (ldap-server)

ldap-server

port (ldap-server)

retransmit (ldap-server)

show ldap server group

timeout (ldap-server)

Command changes Version 5.5.2-1.1: command added

debug ldap client

Overview Use this command to enable LDAP debugging.

Use the **no** variant of this command to disable all LDAP debugging.

Syntax

```
debug ldap client all
debug ldap client {[acl] [args] [ber] [config] [conns] [filter] [packets] [parse] [shell] [stats] [stats2] [sync] [trace]}
no debug ldap client
```

Parameter	Enable or disable debugging for ...
`all`	All LDAP debugging options
`args`	Heavy trace debugging (args, arguments)
`ber`	Print out packets sent and received (ber, Bit Error Rate)
`config`	Configuration processing
`conns`	Connection management
`filter`	Search filter processing
`packets`	Debug packet handling
`parse`	Parsing processing
`shell`	Print communication with shell backends
`stats`	Stats from connections, operations and results
`stats2`	Stats from log entries sent
`sync`	Syncrepl consumer processing (LDAP Sync replication)
`trace`	Trace function calls

Default By default, all LDAP debugging is disabled.

Mode Global Configuration

Example To turn on all LDAP debugging, use the command:

```
awplus# debug ldap client all
```

To turn on filter and packet LDAP debugging, use the command:

```
awplus# debug ldap client filter packets
```

To disable all LDAP debugging, use the command:

```
awplus# no debug ldap client
```

Related commands aaa authentication login

aaa group server

ldap-server

Command changes Version 5.5.2-1.1: command added

group-attribute

Overview Use this command to configure the name of the attribute that group members are stored in.

It is only necessary to set this option if group-dn is used and you don't want to use the default attribute, which is 'uniquemember'.

Use the **no** variant of this command to revert to the default group attribute.

Syntax

```
group-attribute <attribute>
no group-attribute
```

Parameter	Description
<attribute>	The attribute that group members are stored in.

Default The default group attribute is 'uniquemember'.

Mode LDAP Server Configuration

Example To set the group attribute for the LDAP server called 'Server1' to 'member', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# group-attribute member
```

To reset the group attribute to default for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no group-attribute
```

Related commands

base-dn

bind authenticate root-dn

group-dn

ldap-server

login-attribute

search-filter

Command changes Version 5.5.2-1.1: command added

group-dn

Overview Use this command to configure the group DN (Distinguished Name) of the group that users should be a member of.

By default the device will determine this by checking the 'uniquemember' attribute of the group to see if it contains the user's DN string. This can be changed with the group-attribute command.

Use the **no** variant of this command to remove the configured group DN.

Syntax

```
group-dn <group-dn>
no group-dn
```

Parameter	Description
<group-dn>	The DN of the group that users should be a member of.

Default Not set

Mode LDAP Server Configuration

Example To set the group DN for the LDAP server called 'Server1' to 'cn=Users,dc=example, dc=com', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# group-dn cn=Users,dc=example,
dc=com
```

To clear the group DN for 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no group-dn
```

Related commands

base-dn

bind authenticate root-dn

group-attribute

ldap-server

login-attribute

search-filter

Command changes Version 5.5.2-1.1: command added

host (ldap-server)

Overview Use this command to configure the address of the remote LDAP server you want to connect to.

Use the **no** variant of this command to remove the remote LDAP server.

Syntax

```
host {<host-name>|<ip-address>|<ipv6-address>}
no host
```

Parameter	Description
<hostname>	The hostname of the LDAP server.
<ip-address>	The IPv4 address of the LDAP server. Uses the format A.B.C.D.
<ipv6-address>	The IPv6 address of the LDAP server. Uses the format x:x::x:x.

Default Not set

Mode LDAP Server Configuration

Example To set the host for the LDAP server called 'Server1' to the IP address 10.0.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# host 10.0.0.1
```

To set the host for Server1 to the IPv6 address 2001:0db8::a2, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# host 2001:db8::a2
```

To set the host for Server1 to the hostname www.ldapserver.com, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# host www.ldapserver.com
```

To unset the host for Server1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no host
```

Related commands ldap-server

port (ldap-server)

retransmit (ldap-server)

secure mode (ldap-server)

secure cipher (ldap-server)

show ldap server group

secure trustpoint (ldap-server)

timeout (ldap-server)

Command changes

Version 5.5.2-1.1: command added

ldap-server

Overview Use this command to configure an LDAP server and enter LDAP server configuration mode.

Use the **no** variant of this command to remove the specified server.

Syntax

```
ldap-server <server-name>
no ldap-server <server-name>
```

Parameter	Description
<server-name>	The name of the LDAP server.

Default Not set

Mode Global Configuration

Example To create and configure an LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)#
```

To configure the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)#
```

To remove an LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# no ldap-server Server1
```

Related commands

authentication (ldap-server)

host (ldap-server)

port (ldap-server)

retransmit (ldap-server)

secure cipher (ldap-server)

secure mode (ldap-server)

secure trustpoint (ldap-server)

show ldap server group

timeout (ldap-server)

Command changes Version 5.5.2-1.1: command added

login-attribute

Overview Use this command to set the name of the attribute user names are stored in. The device will search this attribute for the user's DN (Distinguished Name).

It is only necessary to set this option if you don't want to use the default attribute, which is 'uid'.

If the authentication method is 'bind-only', then this attribute is used as the first component of the user DN, with the base DN added to complete the user DN.

Use the **no** variant of this command to reset the login attribute to the default of 'uid'.

Syntax

```
login-attribute <attribute>
no login-attribute
```

Parameter	Description
<attribute>	The LDAP attribute to use for the username of connecting users.

Default uid

Mode LDAP Server Configuration

Example To set the login attribute for the LDAP server called 'Server1' to 'sAMAccountName', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# login-attribute sAMAccountName
```

To reset the login attribute for 'Server1' to the default, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no login-attribute
```

Related command

authentication (ldap-server)

base-dn

bind authenticate root-dn

group-attribute

group-dn

ldap-server

search-filter

Command changes Version 5.5.2-1.1: command added

port (ldap-server)

Overview Use this command to configure the port you are using to connect to the remote LDAP server.

Note that if secure ciphers are enabled, then the secure port is used instead. Secure ciphers are configured with the secure mode (ldap-server) command.

Use the **no** variant of this command to reset the port number to the default (389).

Syntax

```
port <1-65535>
no port
```

Parameter	Description
<1-65535>	Port number from 1 through 65535.

Default 389

Mode LDAP Server Configuration

Example To set the port for the LDAP server called 'Server1' to 1579, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# port 1579
```

To reset the port for 'Server1' to the default of 389, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no port
```

Related commands

deadtime (ldap-server)

host (ldap-server)

ldap-server

retransmit (ldap-server)

secure cipher (ldap-server)

secure mode (ldap-server)

secure trustpoint (ldap-server)

show ldap server group

timeout (ldap-server)

Command changes Version 5.5.2-1.1: command added

retransmit (ldap-server)

Overview Use this command to configure the number of times a device will attempt to reconnect to the LDAP server before aborting.

Use the **no** variant of this command to reset the reconnect attempts to the default value of 3.

Syntax

```
retransmit <0-100>
no retransmit
```

Parameter	Description
<0-100>	The number of times the device will attempt to reconnect to the LDAP server.

Default 3 times

Mode LDAP Server Configuration

Example To set the number of reconnect attempts for the LDAP server called 'Server1' to 5 attempts, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# retransmit 5
```

To reset the number of reconnect attempts for 'Server1' to 3 attempts, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no retransmit
```

Related commands

deadtime (ldap-server)

host (ldap-server)

ldap-server

port (ldap-server)

timeout (ldap-server)

Command changes Version 5.5.2-1.1: command added

search-filter

Overview Use this command to add a filter to use when searching for a user on the LDAP server.

The filter should be a form similar to 'attribute=value' or '&(attribute1=value1)(attribute2=value2)

Use the **no** variant of this command to remove the search filter.

Syntax

```
search-filter <filter>
no search-filter
```

Parameter	Description
<filter>	The filter to use when searching for a user.

Default Not set

Mode LDAP Server Configuration

Usage notes If the 'bind-only' authentication method is used, then this value is unused.

For the search authentication method, a search operation is used to search the LDAP server. The client specifies the starting point (base DN) of the search, the search scope (either the object, its children, or the subtree rooted at the object), and a search filter.

Example To set a search filter on the LDAP server called 'Server1' to 'building=block1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# search-filter building=block1
```

To unset the search filter of 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no search-filter
```

Related commands

authentication (ldap-server)

base-dn

bind authenticate root-dn

group-attribute

group-dn

ldap-server

login-attribute

Command changes Version 5.5.2-1.1: command added

secure cipher (ldap-server)

Overview Use this command to configure the OpenSSL ciphers used in LDAP secure mode. You can choose groups of ciphers from a number of Mozilla TLS configs, or specify multiple individual ciphers in OpenSSL format.

Use the **no** variant of this command to remove the configured ciphers on a server.

Syntax

```
secure cipher {old|intermediate|modern}
secure cipher <cipher-list>
no secure cipher
```

Parameter	Description
`old`	Ciphers in Mozilla's old TLS config. Alongside the modern and intermediate ciphers, this includes the following ciphers: DHE-RSA-CHACHA20-POLY1305,ECDHE-ECDSA-AES128SHA256, ECDHE-RSA-AES128-SHA256,ECDHE-ECDSA-AES128-SHA, ECDHE-RSA-AES128-SHA,ECDHE-ECDSA-AES256-SHA384, ECDHE-RSA-AES256-SHA384, ECDHE-ECDSA-AES256-SHA, ECDHE-RSA-AES256-SHA,DHE-RSA-AES128-SHA256, DHE-RSA-AES256-SHA256, AES128-GCM-SHA256, AES256-GCM-SHA384,AES128-SHA256, AES256-SHA256, AES128-SHA, AES256-SHA, DES-CBC3-SHA
`intermediate`	Ciphers in Mozilla's intermediate TLS config. Alongside the modern ciphers, this includes the following ciphers: ECDHE-ECDSA-AES128-GCM-SHA256,ECDHE-RSA-AES128-CM-SHA256, ECDHE-ECDSA-AES256-GCM-SHA384,ECDHE-RSA-AES256-CM-SHA384, ECDHE-ECDSA-CHACHA20-POLY1305,ECDHE-RSA-CHACHA20-POLY1305, DHE-RSA-AES128-GCM-SHA256,DHE-RSA-AES256-GCM-SHA384
`modern`	Ciphers in Mozilla's modern TLS config. Includes the following ciphers: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLY1305_SHA256
<cipher-list>	The name (or names) of a cipher in OpenSSL format. This is a **space** separated list of cipher names, for example: DHE-DSS-AES256-GCM-SHA384 TLS_AES_256_GCM_SHA384

Default Not set

Mode LDAP Server Configuration

Example To use the Intermediate Mozilla cipher suite on the LDAP server called Server1, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure cipher intermediate
```

To remove the configured ciphers on 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no secure cipher
```

To use the ciphers DHE-DSS-AES256-GCM-SHA384 and TLS_AES_256_GCM_SHA384 on 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure cipher
DHE-DSS-AES256-GCM-SHA384 TLS_AES_256_GCM_SHA384
```

Related commands

host (ldap-server)

ldap-server

port (ldap-server)

secure mode (ldap-server)

secure trustpoint (ldap-server)

Command changes

Version 5.5.2-1.1: command added

secure mode (ldap-server)

Overview Use this command to configure the LDAP server to use secure mode. Secure mode encrypts communications with the LDAP server using TLS (Transport Layer Security). If you don't specify a port number, the default port (636) is used.

For secure mode, you should also set the CA certificate using the secure trustpoint (ldap-server) command.

Use **no secure mode** to disable secure mode for communicating with this LDAP server.

Use **no secure mode secure-port** to reset the secure mode port to the default.

Syntax

```
secure mode [secure-port <port>]
no secure mode
no secure mode secure-port
```

Parameter	Description
<port>	The secure port for communicating with the LDAP server

Default Secure mode is disabled, and the default port is 636

Mode LDAP Server Configuration

Example To enable secure mode for communicating with the LDAP server called 'Server1', with the default port, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure mode
```

To disable secure mode for communicating with 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no secure mode
```

To enable secure mode with the port 1234 for communicating with 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# secure mode secure-port 1234
```

To reset the secure mode port to the default on 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no secure mode secure-port
```

Related commands

host (ldap-server)

ldap-server

port (ldap-server)

secure cipher (ldap-server)

secure trustpoint (ldap-server)

Command changes

Version 5.5.2-1.1: command added

secure trustpoint (ldap-server)

Overview Use this command to link a preconfigured trustpoint to the LDAP server configuration. The trustpoint must be the LDAP server certificate and is required to successfully connect to the LDAP server when secure mode is enabled.

Use the **no** variant of this command to remove a trustpoint from an LDAP server.

Syntax

```
secure trustpoint <trustpoint>
no secure trustpoint
```

Parameter	Description
<trustpoint>	The name of the trustpoint used for LDAP secure mode

Default Not set

Mode LDAP Server Configuration

Example To set the trustpoint to Trustpoint1 for the LDAP server called 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap server Server1
awplus(config-ldap-server)# secure trustpoint Trustpoint1
```

To remove the trustpoint from 'Server1', use the commands:

```
awplus# configure terminal
awplus(config)# ldap server Server1
awplus(config-ldap-server)# no secure trustpoint
```

Related commands

host (ldap-server)

ldap-server

port (ldap-server)

secure cipher (ldap-server)

secure mode (ldap-server)

Command changes Version 5.5.2-1.1: command added

server (ldap-group)

Overview Use this command to add an LDAP server to an LDAP server group.

The server is identified by the name of the server, which is created using the ldap-server command.

Use the **no** variant of this command to remove an LDAP server from an LDAP server group.

Syntax

```
server <server-name>
no server <server-name>
```

Parameter	Description
<server-name>	The name of the LDAP server group, specified when creating the LDAP server.

Default By default, LDAP servers are only added to the default 'ldap' server group.

Mode LDAP Server Group Configuration

Usage notes The server is appended to the server list of the group, and the order of configuration determines the precedence of servers.

Example To add the LDAP server called 'Server1' to the LDAP server group called 'Group1', use the commands:

```
awplus# configure terminal
awplus(config)# aaa group server ldap Group1
awplus(config-ldap-group)# server Server1
```

To remove 'Server1' from 'Group1', use the commands:

```
awplus# configure terminal
awplus(config)# aaa group server ldap Group1
awplus(config-ldap-group)# no server Server1
```

Related commands

aaa authentication login

aaa group server

ldap-server

show ldap server group

Command changes Version 5.5.2-1.1: command added

show ldap server group

Overview Use this command to display information about LDAP server groups, their servers and the status of those servers.

Syntax

```
show ldap server group [<group-name>]
```

Parameter	Description
<group-name>	The name of the LDAP server group.

Mode Global Configuration

Usage notes If you specify a single group name, you will only see information relating to that specific server group. Otherwise, all LDAP server groups are shown, including the 'ldap' group that contains every LDAP server.

Example To show all server groups, use the command:

```
awplus# show ldap server group
```

To show the default LDAP group that includes all the LDAP servers, use the command:

```
awplus# show ldap server group ldap
```

To show a server group named 'CustomGroup1', use the command:

```
awplus# show ldap server group CustomGroup1
```

Output Figure 17-1: Example output from **show ldap server group**

```
LDAP Group Configuration
 Group Name : ldap
  LDAP server name    Server Host/IP Address      Port  Status
-------------------------------------------------------------------
 server_one           10.1.1.1                    N/A   Alive
 server_two           10.2.1.1                    N/A   Dead (1 hour)

Group Name : CustomGroup1
  LDAP server name    Server Host/IP Address      Port  Status
-------------------------------------------------------------------
 server_one           10.1.1.1                    N/A   Alive

Group Name : CustomGroup2
  LDAP server name    Server Host/IP Address      Port  Status
-------------------------------------------------------------------
  No LDAP servers currently defined
```

Related commands

aaa authentication login

aaa group server

deadtime (ldap-server)

ldap-server

port (ldap-server)

server (ldap-group)

Command changes Version 5.5.2-1.1: command added

timeout (ldap-server)

Overview Use this command to set the time to wait for a connection before reattempting to connect to the LDAP server.

Use the **no** variant of this command to reset the timeout back to the default value.

Syntax

```
timeout <1-1000>
no timeout
```

Parameter	Description
<1-1000>	The number of seconds to wait for a connection before reattempting to connect to the LDAP server.

Default 5 seconds

Mode LDAP Server Configuration

Example To set the server timeout for the LDAP server called 'Server1' to 10 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# timeout 10
```

To set the server timeout for 'Server1' to the default, use the commands:

```
awplus# configure terminal
awplus(config)# ldap-server Server1
awplus(config-ldap-server)# no timeout
```

Related commands

deadtime (ldap-server)

host (ldap-server)

ldap-server

port (ldap-server)

retransmit (ldap-server)

Command changes Version 5.5.2-1.1: command added

18 RADIUS Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure the device as a RADIUS client.

For more information, see the RADIUS Feature Overview and Configuration Guide.

Command List

- "auth-mac-promiscuous" on page 492
- "deadtime (RADIUS server group)" on page 493
- "debug radius" on page 494
- "ip radius require-message-authenticator" on page 495
- "ip radius source-interface" on page 496
- "radius-server deadtime" on page 497
- "radius-server host" on page 498
- "radius-server key" on page 501
- "radius-server retransmit" on page 502
- "radius-server timeout" on page 504
- "server (RADIUS server group)" on page 506
- "show debugging radius" on page 508
- "show radius" on page 509
- "show radius local-server auth-mac-promiscuous" on page 512
- "undebug radius" on page 513

auth-mac-promiscuous

Overview Use this command to enable promiscuous mode for MAC address authentication on a local RADIUS server.

Use the **no** variant of this command to disable MAC authentication promiscuous mode on a local RADIUS server.

Syntax

```
auth-mac-promiscuous
no auth-mac-promiscuous
```

Default Disabled.

Mode RADIUS Server Configuration

Usage notes In promiscuous mode, the RADIUS server will respond with an Access-Accept for any Access-Request with a Radius Service-Type attribute of 'Call-Check', when the supplicants credentials are NOT in the user database.

If the credentials do appear in the database, the behavior of the server is unchanged.

Example To disable MAC authentication promiscuous mode on a local RADIUS server, use the commands:

```
awplus# radius-server local
awplus(config-radsrv)# no auth-mac-promiscuous
```

Related commands show radius local-server auth-mac-promiscuous

Command changes Version 5.5.3-2.1: command added

deadtime (RADIUS server group)

Overview Use this command to configure the **deadtime** parameter for the RADIUS server group. This command overrides the global dead-time configured by the radius-server deadtime command. The configured deadtime is the time period in minutes to skip a RADIUS server for authentication or accounting requests if the server is 'dead'. Note that a RADIUS server is considered 'dead' if there is no response from the server within a defined time period.

Use the **no** variant of this command to reset the deadtime configured for the RADIUS server group. If the global deadtime for RADIUS server is configured the value will be used for the servers in the group. The global deadtime for the RADIUS server is set to 0 minutes by default.

Syntax

```
deadtime <0-1440>
no deadtime
```

Parameter	Description
<0-1440>	Amount of time in minutes.

Default The deadtime is set to 0 minutes by default.

Mode RADIUS Server Group Configuration

Usage If the RADIUS server does not respond to a request packet, the packet is retransmitted the number of times configured for the **retransmit** parameter (after waiting for a **timeout** period to expire). The server is then marked 'dead', and the time is recorded. The **deadtime** parameter configures the amount of time to skip a dead server; if a server is dead, no request message is sent to the server for the **deadtime** period.

Examples To configure the deadtime for 5 minutes for the RADIUS server group 'GROUP1', use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1
awplus(config-sg)# deadtime 5
```

To remove the deadtime configured for the RADIUS server group 'GROUP1', use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no deadtime
```

Related commands aaa group server

radius-server deadtime

debug radius

Overview This command enables RADIUS debugging. If no option is specified, all debugging options are enabled.

Use the **no** variant of this command to disable RADIUS debugging. If no option is specified, all debugging options are disabled.

Syntax

```
debug radius [packet|event|all]
no debug radius [packet|event|all]
```

Parameter	Description
`packet`	Debugging for RADIUS packets is enabled or disabled.
`event`	Debugging for RADIUS events is enabled or disabled.
`all`	Enable or disable all debugging options.

Default RADIUS debugging is disabled by default.

Mode Privileged Exec

Examples To enable debugging for RADIUS packets, use the command:

```
awplus#  debug radius packet
```

To enable debugging for RADIUS events, use the command:

```
awplus#  debug radius event
```

To disable debugging for RADIUS packets, use the command:

```
awplus# no debug radius packet
```

To disable debugging for RADIUS events, use the command:

```
awplus# no debug radius event
```

Related commands show debugging radius

undebug radius

ip radius require-message-authenticator

Overview Use this command to configure the RADIUS client to reject unverified RADIUS packets. This means it will discard any received RADIUS Access-Accept, Access-Challenge, and Access-Reject packets that do not have a valid Message-Authenticator attribute.

Use the **no** variant of this command to allow the client to accept unverified RADIUS packets.

Syntax

```
ip radius require-message-authenticator
no ip radius require-message-authenticator
```

Default Disabled

Mode Global Configuration

Example To require Message-Authenticator attributes in responses from RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# ip radius require-message-authenticator
```

Related commands radius-server host

Command changes Version 5.5.4-2.3: command added

ip radius source-interface

Overview This command configures the source IP address of every outgoing RADIUS packet to use a specific IP address or the IP address of a specific interface. If the specified interface is down or there is no IP address on the interface, then the source IP address of outgoing RADIUS packets depends on the interface the packets leave.

Use the **no** variant of this command to remove the source interface configuration. The source IP address in outgoing RADIUS packets will be the IP address of the interface from which the packets are sent.

Syntax

```
ip radius source-interface {<interface>|<ip-address>}
no ip radius source-interface
```

Parameter	Description
<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 eth0 for the source IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface eth0
```

To configure the source IP address of all outgoing RADIUS packets to use 192.168.1.10, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface 192.168.1.10
```

To reset the source interface configuration for all outgoing RADIUS packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip radius source-interface
```

Related commands radius-server host

radius-server deadtime

Overview Use this command to specify the global **deadtime** for all RADIUS servers. If a RADIUS server is considered dead, it is skipped for the specified deadtime. This command specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

Use the **no** variant of this command to reset the global deadtime to the default of 0 seconds, so that RADIUS servers are not skipped even if they are dead.

Syntax

```
radius-server deadtime <minutes>
no radius-server deadtime
```

Parameter	Description
<minutes>	RADIUS server deadtime in minutes in the range 0 to 1440 (24 hours).

Default The default RADIUS deadtime configured on the system is 0 seconds.

Mode Global Configuration

Usage The RADIUS client considers a RADIUS server to be dead if it fails to respond to a request after it has been retransmitted as often as specified globally by the radius-server retransmit command or for the server by the radius-server host command. To improve RADIUS response times when some servers may be unavailable, set a **deadtime** to skip dead servers.

Examples To set the dead time of the RADIUS server to 60 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server deadtime 60
```

To disable the dead time of the RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server deadtime
```

Related commands

deadtime (RADIUS server group)

radius-server host

radius-server retransmit

radius-server host

Overview Use this command to specify a remote RADIUS server host for authentication or accounting, and to set server-specific parameters. The parameters specified with this command override the corresponding global parameters for RADIUS servers. This command specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination UDP port numbers.

This command adds the RADIUS server address and sets parameters to the RADIUS server. The RADIUS server is added to the running configuration after you issue this command. If parameters are not set using this command then common system settings are applied.

Use the **no** variant of this command to remove the specified server host as a RADIUS authentication and/or accounting server and set the destination port to the default RADIUS server port number (1812).

Syntax

```
radius-server host {<host-name>|<ip-address>} [acct-port
<0-65535>] [auth-port <0-65535>] [key <key-string>] [retransmit
<0-100>] [timeout <1-1000>]
```

```
no radius-server host {<host-name>|<ip-address>} [acct-port
<0-65535>] [auth-port <0-65535>]
```

Parameter	Description
<host-name>	Server host name. The DNS name of the RADIUS server host.
<ip-address>	The IP address of the RADIUS server host.
`acct-port`	Accounting port. Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the server is not used for accounting. The default UDP port for accounting is 1813.
<0-65535>	UDP port number. (Accounting port number is set to (accounting port number is set to 1813 by default) Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the host is not used for accounting.
`auth-port`	Authentication port. Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the server is not used for authentication. The default UDP port for authentication is 1812.
<0-65535>	UDP port number (authentication port number is set to 1812 by default). Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the host is not used for authentication.
`timeout`	Specifies the amount of time to wait for a response from the server. If this parameter is not specified the global value configured by the **radius-server timeout** command is used.

Parameter	Description
<1-1000>	Time in seconds to wait for a server reply (timeout is set to 5 seconds by default). The time interval (in seconds to wait for the RADIUS server to reply before retransmitting a request or considering the server dead. This setting overrides the global value set by the **radius-server timeout** command. If no timeout value is specified for this server, the global value is used.
`retransmit`	Specifies the number of retries before skip to the next server. If this parameter is not specified the global value configured by the **radius-server retransmit** command is used.
<0-100>	Maximum number of retries (maximum number of retries is set to 3 by default). The maximum number of times to resend a RADIUS request to the server, if it does not respond within the timeout interval, before considering it dead and skipping to the next RADIUS server. This setting overrides the global setting of the **radius-server retransmit** command. If no retransmit value is specified, the global value is used.
`key`	Set shared secret key with RADIUS servers.
<key-string>	Shared key string applied. Specifies the shared secret authentication or encryption key for all RADIUS communications between this device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the string are used. 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 **radius-server key** command. If no key value is specified, the global value is used.

Default The RADIUS client address is not configured (null) by default. No RADIUS server is configured.

Mode Global Configuration

Usage Multiple **radius -server host** commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host. If there are multiple RADIUS servers for this client, use this command multiple times—once to specify each server.

If you specify a host without specifying the auth port or the acct port, it will by default be configured for both authentication and accounting, using the default UDP ports. To set a host to be a RADIUS server for authentication requests only, set the **acct-port** parameter to 0; to set the host to be a RADIUS server for accounting requests only, set the auth-port parameter to 0.

A RADIUS server is identified by IP address, authentication port and accounting port. A single host can be configured multiple times with different authentication or accounting ports. All the RADIUS servers configured with this command are included in the predefined RADIUS server group radius, which may be used by AAA authentication, authorization and accounting commands. The client transmits

(and retransmits, according to the **retransmit** and **timeout** parameters) RADIUS authentication or accounting requests to the servers in the order you specify them, until it gets a response.

Examples To add the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20
```

To set the secret key to 'mySecret' on the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 key mySecret
```

To delete the RADIUS server 10.0.0.20, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host 10.0.0.20
```

To configure rad1.company.com for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad1.company.com acct-port 0
```

To remove the RADIUS server rad1.company.com configured for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host rad1.company.com
acct-port 0
```

To configure rad2.company.com for accounting only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad2.company.com auth-port 0
```

To configure 192.168.1.1 with authentication port 1000, accounting port 1001 and retransmit count 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 192.168.1.1 auth-port 1000
acct-port 1001 retransmit 5
```

Related commands

aaa group server

radius-server key

radius-server retransmit

radius-server timeout

Command changes

Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

Version 5.4.9-2.1: **key-encrypted** parameter added

radius-server key

Overview This command sets a global secret key for RADIUS authentication on the device. The shared secret text string is used for RADIUS authentication between the device and a RADIUS server.

Note that if no secret key is explicitly specified for a RADIUS server, the global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to reset the secret key to the default (null).

Syntax

```
radius-server key <key-string>
no radius-server key
```

Parameter	Description
<key-string>	Shared secret among RADIUS server and 802.1X client.

Default The RADIUS server secret key on the system is not set by default (null).

Mode Global Configuration

Usage Use this command to set the global secret key shared between this client and its RADIUS servers. If no secret key is specified for a particular RADIUS server using the **radius-server host** command, this global key is used.

After enabling AAA authentication with the **aaa authentication login** command, set the authentication and encryption key using the **radius-server key** command so the key entered matches the key used on the RADIUS server.

Examples To set the global secret key to **allied** for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server key allied
```

To set the global secret key to **secret** for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server key secret
```

To delete the global secret key for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server key
```

Related commands radius-server host

radius-server retransmit

Overview This command sets the retransmit counter to use RADIUS authentication on the device. This command specifies how many times the device transmits each RADIUS request to the RADIUS server before giving up.

This command configures the **retransmit** parameter for RADIUS servers globally. If the **retransmit** parameter is not specified for a RADIUS server by the **radius-server host** command then the global configuration set by this command is used for the server instead.

Use the **no** variant of this command to reset the re-transmit counter to the default (3).

Syntax

```
radius-server retransmit <retries>
no radius-server retransmit
```

Parameter	Description
<retries>	RADIUS server retries in the range <0-100>. The number of times a request is resent to a RADIUS server that does not respond, before the server is considered dead and the next server is tried. If no retransmit value is specified for a particular RADIUS server using the **radius-server host** command, this global value is used.

Default The default RADIUS retransmit count on the device is 3.

Mode Global Configuration

Examples To set the RADIUS **retransmit** count to 1, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 1
```

To set the RADIUS **retransmit** count to the default (3), use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server retransmit
```

To configure the RADIUS **retransmit** count globally with 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 5
```

To disable retransmission of requests to a RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 0
```

Related commands

radius-server deadtime

radius-server host

radius-server timeout

Overview Use this command to specify the RADIUS global timeout value. This is how long the device waits for a reply to a RADIUS request before retransmitting the request, or considering the server to be dead. If no timeout is specified for the particular RADIUS server by the **radius-server host** command, it uses this global timeout value.

Note that this command configures the **timeout** parameter for RADIUS servers globally.

The **no** variant of this command resets the transmit timeout to the default (5 seconds).

Syntax

```
radius-server timeout <seconds>
no radius-server timeout
```

Parameter	Description
<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 **radius-server retransmit** command).

Default The default RADIUS transmit timeout on the system is 5 seconds.

Mode Global Configuration

Examples To globally set the device to wait 20 seconds before retransmitting a RADIUS request to unresponsive RADIUS servers, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 20
```

To set the RADIUS **timeout** parameter to 1 second, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 1
```

To set the RADIUS **timeout** parameter to the default (5 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server timeout
```

To configure the RADIUS server **timeout** period globally with 3 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 3
```

To reset the global **timeout** period for RADIUS servers to the default, use the following command:

```
awplus# configure terminal
awplus(config)# no radius-server timeout
```

Related commands

radius-server deadtime

radius-server host

radius-server retransmit

server (RADIUS server group)

Overview This command adds a RADIUS server to a server group in RADIUS Server Group Configuration mode. The RADIUS server should be configured by the radius-server host command.

The device adds each server to the end of the group's list of servers, so add the servers in order of priority. If you add a server and it is already in the list, it will be removed and then re-added to the end of the list.

The server is identified by IP address and authentication and accounting UDP port numbers. So a RADIUS server can have multiple entries in a group with different authentication and/or accounting UDP ports. The **auth-port** specifies the UDP destination port for authentication requests to the server. To disable authentication for the server, set **auth-port** to 0. If the authentication port is missing, the default port number is 1812. The **acct-port** specifies the UDP destination port for accounting requests to the server. To disable accounting for the server, set **acct-port** to 0. If the accounting port is missing, the default port number is 1813.

Use the **no** variant of this command to remove a RADIUS server from the server group.

Syntax

```
server {<hostname>|<ip-address>} [auth-port <0-65535>]
[acct-port <0-65535>]
```

```
no server {<hostname>|<ip-address>} [auth-port <0-65535>]
[acct-port <0-65535>]
```

Parameter	Description
<hostname>	Server host name
<ip-address>	Server IP address 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 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.
<0-65535>	UDP port number (default: 1812)
acct-port	Accounting port 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.
<0-65535>	UDP port number (default: 1813)

Default The default Authentication port number is 1812 and the default Accounting port number is 1813.

Mode RADIUS Server Group Configuration

Usage notes The RADIUS server to be added must be configured by the **radius-server host** command. In order to add or remove a server, the **auth-port** and **acct-port** parameters in this command must be the same as the corresponding parameters in the **radius-server host** command.

Examples To create a RADIUS server group 'RAD_AUTH1' for authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_AUTH1
awplus(config-sg)# server 192.168.1.1 acct-port 0
awplus(config-sg)# server 192.168.2.1 auth-port 1000 acct-port
0
```

To create a RADIUS server group 'RAD_ACCT1' for accounting, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_ACCT1
awplus(config-sg)# server 192.168.2.1 auth-port 0 acct-port
1001
awplus(config-sg)# server 192.168.3.1 auth-port 0
```

To remove server 192.168.3.1 from the existing server group 'GROUP1', use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no server 192.168.3.1
```

Related commands

aaa accounting login

aaa authentication login

aaa group server

radius-server host

show debugging radius

Overview This command displays the current debugging status for the RADIUS servers.

Syntax

```
show debugging radius
```

Mode User Exec and Privileged Exec

Example To display the current debugging status of RADIUS servers, use the command:

```
awplus# show debugging radius
```

Output Figure 18-1: 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 18-2: 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 18-3: Example output from the **show radius** command showing RADIUS client status

```
RADIUS global interface name: awplus
 Secret key:
 Timeout: 5
 Retransmit count: 3
 Deadtime: 0

Server Address: 150.87.18.89
 Auth destination port: 1812
 Accounting port: 1813
 Secret key: swg
 Timeout: 5
 Retransmit count: 3
 Deadtime: 0
```

Output Parameter	Meaning
Source Interface	The interface name or IP address to be used for the source address of all outgoing RADIUS packets.
Secret Key	A shared secret key to a radius server.
Timeout	A time interval in seconds.
Retransmit Count	The number of retry count if a RADIUS server does not response.
Deadtime	A time interval in minutes to mark a RADIUS server as “dead”.
Interim-Update	A time interval in minutes to send Interim-Update Accounting report.
Group Deadtime	The deadtime configured for RADIUS servers within a server group.
Server Host	The RADIUS server hostname or IP address.
Authentication Port	The destination UDP port for RADIUS authentication requests.
Accounting Port	The destination UDP port for RADIUS accounting requests.

Output Parameter	Meaning	
`Auth Status`	The status of the authentication port. 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. The status ("dead", "error", or "alive") of the RADIUS accounting server and, if dead, how long it has been dead for.	

show radius local-server auth-mac-promiscuous

Overview Use this command to show the status of the **auth-mac-promiscuous** command.

Syntax

```
show radius local-server auth-mac-promiscuous
```

Mode User Exec

Usage notes In promiscuous mode, the RADIUS server will respond with an Access-Accept for any Access-Request with a Radius Service-Type attribute of 'Call-Check', when the supplicants credentials are NOT in the user database.

If the credentials do appear in the database, the behavior of the server is unchanged.

Example To display the status of the **auth-mac-promiscuous** command, use the command:

```
awplus# show radius local-server auth-mac-promiscuous
```

Output Figure 18-4: Example output from **show radius local-server auth-mac-promiscuous**

```
awplus#show radius local-server auth-mac-promiscuous
Auth-mac promiscuous mode: Disabled
...
```

Related commands auth-mac-promiscuous

Command changes Version 5.5.3-2.1: command added

undebug radius

Overview This command applies the functionality of the **no** debug radius command.

19 Public Key Infrastructure and Crypto Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure the Public Key Infrastructure (PKI) capabilities on an AlliedWare Plus device. For more information about PKI, see the Public Key Infrastructure (PKI) Feature Overview and Configuration Guide.

Command List

- "crypto key generate rsa" on page 516
- "crypto key zeroize" on page 517
- "crypto pki authenticate" on page 518
- "crypto pki enroll" on page 519
- "crypto pki enroll user" on page 520
- "crypto pki export pem" on page 522
- "crypto pki export pkcs12" on page 523
- "crypto pki import pem" on page 525
- "crypto pki import pkcs12" on page 527
- "crypto pki trustpoint" on page 528
- "enrollment (ca-trustpoint)" on page 529
- "fingerprint (ca-trustpoint)" on page 530
- "no crypto pki certificate" on page 532
- "rsakeypair (ca-trustpoint)" on page 533
- "show crypto key mypubkey rsa" on page 534
- "show crypto pki certificates" on page 535
- "show crypto pki enrollment user" on page 537
- "show crypto pki trustpoint" on page 538
- "show hash" on page 539

- "subject-name (ca-trustpoint)" on page 540

crypto key generate rsa

Overview Use this command to generate a cryptographic public/private key pair for the Rivest-Shamir-Adleman (RSA) encryption algorithm.

Syntax

```
crypto key generate rsa [label <keylabel>] [<1024-16384>]
```

Parameter	Description
`label`	Specify and optional label for the key.
<keylabel>	The name of the key to be created. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters. If no label is specified the default value “server-default” is used.
<1024-16384>	The bit length for the key. If no bit length is specified the default of 2048 is used.

Mode Privileged Exec

Usage notes The generated key may be used for multiple server certificates in the system. A key is referenced by its label. A bit length between 1024 and 16384 bits may be specified. Larger bit lengths are more secure, but require more computation time.

The specified key must not already exist.

Example To create a key with the label ‘example-server-key’ and a bit length of 4096, use the commands:

```
awplus> enable
awplus# crypto key generate rsa label example-server-key 4096
```

Related commands

crypto key zeroize

rsakeypair (ca-trustpoint)

show crypto key mypubkey rsa

Command changes Version 5.5.2-2.1: Key length increased to 16384

crypto key zeroize

Overview Use this command to delete one or all cryptographic public/private key pairs.

Syntax

```
crypto key zeroize rsa <keylabel>
crypto key zeroize all
```

Parameter	Description
`rsa <keylabel>`	Delete a single key pair for the Rivest-Shamir-Adleman (RSA) encryption algorithm.
`all`	Delete all keys.

Mode Privileged Exec

Usage notes Note that this command has the same effect as using the **delete** command (it deletes the file from Flash memory but does not overwrite it with zeros).

The specified key must exist but must not be in use for any existing server certificates.

A key may not be deleted if it is associated with the server certificate or server certificate signing request for an existing trustpoint. To remove a server certificate so that the key may be deleted, use the **no crypto pki enroll** command to de-enroll the server.

Example To delete an RSA key named "example-server-key", use the following command:

```
awplus# crypto key zeroize rsa example-server-key
```

Related commands crypto key generate rsa

show crypto key mypubkey rsa

Command changes Version 5.4.6-1.1: zeroize functionality added to x930 Series

Version 5.4.8-1.2: zeroize functionality added to x220, XS900MX, x550 Series

Version 5.4.8-2.1: zeroize functionality added to SBx908 GEN2, x950 Series

crypto pki authenticate

Overview Use this command to authenticate a trustpoint by generating or importing the root CA certificate. This must be done before the server can be enrolled to the trustpoint.

Syntax

```
crypto pki authenticate <trustpoint>
```

Parameter	Description
<trustpoint>	The name of the trustpoint to be authenticated.

Mode Privileged Exec

Usage notes If the trustpoint's **enrollment** setting is "selfsigned", then this command causes a private key to be generated for the root CA, and a self-signed certificate to be generated based on that key.

If the trustpoint's **enrollment** setting is "terminal", then this command prompts the user to paste a certificate Privacy Enhanced Mail (PEM) file at the CLI terminal. If the certificate is a valid selfsigned CA certificate, then it will be stored as the trustpoint's root CA certificate.

The specified trustpoint must already exist, and its enrollment mode must have been defined.

Example To show the **enrollment** setting of a trustpoint named "example" and then generate a certificate from it, use the commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# enrollment selfsigned
awplus(config)# exit
awplus# exit
awplus# crypto pki authenticate example
```

Related commands

crypto pki import pem

crypto pki trustpoint

enrollment (ca-trustpoint)

crypto pki enroll

Overview Use this command to enroll the local server to the specified trustpoint.

Use the **no** variant of this command to de-enroll the server by removing its certificate

Syntax

```
crypto pki enroll <trustpoint>
no crypto pki enroll <trustpoint>
```

Parameter	Description
<trustpoint>	The name of the trustpoint to be enrolled

Mode Privileged Exec

Usage notes For the local server, "enrollment" is the process of creating of a certificate for the server that has been signed by a CA associated with the trustpoint. The public portion of the RSA key pair specified using the rsakeypair parameter for the trustpoint will be included in the server certificate.

If the trustpoint represents a locally self-signed certificate authority, then this command results in the direct generation of the server certificate, signed by the root CA for the trustpoint.

If the trustpoint represents an external certificate authority, then this command results in the generation of a Certificate Signing Request (CSR) file, which is displayed at the terminal in Privacy-Enhanced Mail (PEM) format, suitable for copying and pasting into a file or message. The CSR must be sent to the external CA for processing. When the CA replies with the signed certificate, that certificate should be imported using the crypto pki import pem command, to complete the enrollment process.

The specified trustpoint must already exist, and it must already be authenticated.

Example To enroll the local server with the trustpoint "example", use the following commands:

```
awplus> enable
awplus# crypto pki enroll example
```

Related commands

crypto pki enroll user

crypto pki import pem

crypto pki trustpoint

enrollment (ca-trustpoint)

crypto pki enroll user

Overview Use this command to enroll a single RADIUS user or all RADIUS users to the specified trustpoint.

Use the **no** variant of this command to remove the PKCS#12 file from the system. Note that the PKCS#12 files are generated in a temporary (volatile) file system, so a system restart also results in removal of all of the files.

Syntax

```
crypto pki enroll <trustpoint>
{user <username>|local-radius-all-users}
```

```
no crypto pki enroll <trustpoint>
{user <username>|local-radius-all-users}
```

Parameter	Description
<trustpoint>	The name of the trustpoint to which users are to be enrolled.
<username>	The name of the user to enroll to the trustpoint.

Mode Privileged Exec

Usage notes For RADIUS users, “enrollment” is the process of generating a private key and a corresponding client certificate for each user, with the certificate signed by the root CA for the trustpoint. The resulting certificates may be exported to client devices, for use with PEAP or EAP-TLS authentication with the local RADIUS server.

The specified trustpoint must represent a locally self-signed certificate authority.

The private key and certificate are packaged into a PKCS#12-formatted file, suitable for export using the **crypto pki export pkcs12** command. The private key is encrypted for security, with a passphrase that is entered at the command line. The passphrase is required when the PKCS#12 file is imported on the client system. The passphrase is not stored anywhere on the device, so users are responsible for remembering it until the export-import process is complete.

If **local-radius-all-users** is specified instead of an individual user, then keys and certificates for all RADIUS users will be generated at once. All the keys will be encrypted using the same passphrase.

The specified trustpoint must already exist, it must represent a locally self-signed CA, and it must already have been authenticated.

Example To enroll the user “example-user” with the trustpoint “example”, use the following commands:

```
awplus> enable
```

```
awplus# crypto pki enroll example user example-user
```

To enroll all local RADIUS users with the trustpoint “example”, use the following commands:

```
awplus> enable
awplus# crypto pki enroll example local-radius-all-users
```

Related commands

crypto pki export pkcs12

crypto pki trustpoint

crypto pki export pem

Overview Use this command to export the root CA certificate for the given trustpoint to a file in Privacy-Enhanced Mail (PEM) format. The file may be transferred to the specified destination URL, or displayed at the terminal.

Syntax

```
crypto pki export <trustpoint> pem [terminal|<url>]
```

Parameter	Description
<trustpoint>	The name of the trustpoint for which the root CA certificate is to be exported.
terminal	Display the PEM file to the terminal.
<url>	Transfer the PEM file to the specified URL.

Default The PEM will be displayed to the terminal by default.

Mode Privileged Exec

Usage notes The specified trustpoint must already exist, and it must already be authenticated.

Example To display the PEM file for the trustpoint “example” to the terminal, use the following commands:

```
awplus> enable
awplus# crypto pki export example pem terminal
```

To export the PEM file “example.pem” for the trustpoint “example” to the URL “tftp://server_a/”, use the following commands:

```
awplus> enable
awplus# crypto pki export example pem
tftp://server_a/example.pem
```

Related commands

crypto pki authenticate

crypto pki import pem

crypto pki trustpoint

crypto pki export pkcs12

Overview Use this command to export a certificate and private key for an entity in a trustpoint to a file in PKCS#12 format at the specified URL. The private key is encrypted with a passphrase for security.

Syntax

```
crypto pki export <trustpoint> pkcs12 {ca|server|<username>}
<url>
```

Parameter	Description
<trustpoint>	The name of the trustpoint for which the certificate and key are tobe exported.
`ca`	If this option is specified, the command exports the root CA certificate and corresponding key.
`server`	If this option is specified, the command exports the server certificate and corresponding key.
<username>	If a RADIUS username is specified, the command exports the PKCS#12 file that was previously generated using the crypto pki enroll user command. To avoid ambiguity with keywords, the username may be prefixed by the string “user:”.
<url>	The destination URL for the PKCS#12 file. The format of the URLis the same as any valid destination for a file copy command.

Mode Privileged Exec

Usage notes If the **ca** option is specified, this command exports the root CA certificate and the corresponding private key, if the trustpoint has been authenticated as a locally selfsigned CA. (If the trustpoint represents an external CA, then there is no private key on the system corresponding to the root CA certificate. Use the **crypto pki export pem** file to export the certificate by itself.) The command prompts for a passphrase to encrypt the private key.

If the **server** option is specified, this command exports the server certificate and the corresponding private key, if the server has been enrolled to the trustpoint. The command prompts for a passphrase to encrypt the private key.

If a RADIUS username is specified, this command exports the PKCS#12 file that was generated using the **crypto pki enroll user** command. (The key within the file was already encrypted as part of the user enrollment process.)

In the event that there is a RADIUS user named “ca” or “server”, enter “user:ca” or “user:server” as the username.

The key and certificate must already exist.

Example To export the PKCS#12 file "example.pk12" for the trustpoint "example" to the URL "tftp://backup/", use the following commands:

```
awplus> enable

awplus# crypto pki export example pkcs12 ca
tftp://backup/example.pk12
```

Related commands

crypto pki enroll user

crypto pki export pem

crypto pki import pkcs12

crypto pki import pem

Overview This command imports a certificate for the given trustpoint from a file in Privacy-Enhanced Mail (PEM) format. The file may be transferred from the specified destination URL, or entered at the terminal.

Syntax

```
crypto pki import <trustpoint> pem [terminal|<url>]
```

Parameter	Description
<trustpoint>	The name of the trustpoint for which the root CA certificate is to be imported.
terminal	Optional parameter, If specified, the command prompts the user to enter (or paste) the PEM file at the terminal. If parameter is specified terminal is assumed by default.
<url>	Optional parameter, If specified, the PEM file is transferred from the specified URL

Default The PEM will be imported from the terminal by default.

Mode Privileged Exec

Usage notes The command is generally used for trustpoints representing external certificate authorities. It accepts root CA certificates, intermediate CA certificates, and server certificates. The system automatically detects the certificate type upon import.

Using this command to import root CA certificates at the terminal is identical to the functionality provided by the crypto pki authenticate command, for external certificate authorities. The imported certificate is validated to ensure it is a proper CA certificate.

Intermediate CA certificates are validated to ensure they are proper CA certificates, and that the issuer chain ends in a root CA certificate already installed for the trustpoint. If there is no root CA certificate for the trustpoint (i.e., if the trustpoint is unauthenticated) then intermediate CA certificates may not be imported.

Server certificates are validated to ensure that the issuer chain ends in a root CA certificate already installed for the trustpoint. If there is no root CA certificate for the trustpoint (i.e., if the trustpoint is unauthenticated) then server certificates may not be imported.

The specified trustpoint must already exist. If the imported certificate is self-signed, then no certificates may exist for the trustpoint. Otherwise, the issuer's certificate must already be present for the trustpoint.

Example To import the PEM file for the trustpoint "example" from the terminal, use the following commands:

```
awplus> enable
awplus# crypto pki import example pem
```

To import the PEM file for the trustpoint "example" from the URL "tftp://server_a/", use the following commands:

```
awplus> enable

awplus# crypto pki import example pem
tftp://server_a/example.pem
```

Related commands

crypto pki authenticate

crypto pki export pem

crypto pki trustpoint

crypto pki import pkcs12

Overview This command imports a certificate and private key for an entity in a trustpoint from a file in PKCS#12 format at the specified URL. The command prompts for a passphrase to decrypt the private key within the file.

Syntax

```
crypto pki import <trustpoint> pkcs12 {ca|server} <url>
```

Parameter	Description
<trustpoint>	The name of the trustpoint for which the certificate and key are to be imported.
ca	If this option is specified, the command imports the root CA certificate and corresponding key.
server	If this option is specified, the command imports the server certificate and corresponding key.
<url>	The source URL for the PKCS#12 file. The format of the URLis the same as any valid destination for a file copy command.

Mode Privileged Exec

Usage notes If the **ca** option is specified, this command imports the root CA certificate and the corresponding private key. This is only valid if the root CA certificate does not already exist for the trustpoint (i.e., if the trustpoint is unauthenticated).

If the **server** option is specified, this command imports the server certificate and the corresponding private key. The imported private key is given a new unique label of the form "localN", where N is a non-negative integer. This operation is only valid if the server certificate does not already exist for the trustpoint (i.e., if the server is not enrolled to the trustpoint).

PKCS#12 files for RADIUS users may not be imported with this command. (There is no value in doing so, as the files are not needed on the local system.)

The specified trustpoint must already exist. The key and certificate must not already exist.

Example To import the PKCS#12 file "example.pk12" for the trustpoint "example" to the URL "tftp://backup/", use the following commands:

```
awplus> enable
awplus# crypto pki import example pkcs12 ca
tftp://backup/example.pk12
```

Related commands

crypto pki export pkcs12

crypto pki import pem

crypto pki trustpoint

Overview Use this command to declare the named trustpoint and enter trustpoint configuration mode.

Use the **no** variant of this command to destroy the trustpoint.

Syntax

```
crypto pki trustpoint <trustpoint>
no crypto pki trustpoint <trustpoint>
```

Parameter	Description
<trustpoint>	The name of the trustpoint. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters.

Mode Global Configuration

Usage notes If the trustpoint did not previously exist, it is created as a new trustpoint. The trustpoint will be empty (unauthenticated) unless the name "local" is selected, in which case the system will automatically authenticate the trustpoint as a local self-signed certificate authority.

The **no** variant of this command destroys the trustpoint by removing all CA and server certificates associated with the trustpoint, as well as the private key associated with the root certificate (if the root certificate was locally self-signed). This is a destructive and irreversible operation, so this command should be used with caution.

Example To configure a trustpoint named "example", use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
```

Related commands show crypto pki certificates

show crypto pki trustpoint

Command changes Version 5.4.6-1.1: command added to x930 Series

Version 5.4.8-1: command added to x220, XS900MX, x550 Series

Version 5.4.8-2.1: command added to SBx908 GEN2, x950 Series

enrollment (ca-trustpoint)

Overview Use this command to declare how certificates will be added to the system for the current trustpoint.

Syntax

```
enrollment {selfsigned|terminal}
```

Parameter	Description
`selfsigned`	Sets the enrollment mode for the current trustpoint to selfsigned.
`terminal`	Sets the enrollment mode for the current trustpoint to terminal.

Mode Trustpoint Configuration

Usage notes If the enrollment is set to **selfsigned**, then the system will generate a root CA certificate and its associated key when the **crypto pki authenticate** command is issued. It will generate a server certificate (signed by the root CA certificate) when the **crypto pki enroll** command is issued.

If the enrollment is set to **terminal**, then the system will prompt the user to paste the root CA certificate Privacy Enhanced Mail (PEM) file at the terminal, when the **crypto pki authenticate** command is issued. It will create a Certificate Signing Request (CSR) file for the local server when the **crypto pki enroll** command is issued. The server certificate received from the external CA should be imported using the **crypto pki import pem** command.

The trustpoint named “local” may only use the **selfsigned** enrollment setting.

If no enrollment mode is specified, the **crypto pki authenticate** command will fail for the trustpoint.

Example To configure the trustpoint named "example" and set its enrollment to **selfsigned**, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# enrollment selfsigned
```

Related commands crypto pki enroll

fingerprint (ca-trustpoint)

Overview Use this command to declare that certificates with the specified fingerprint should be automatically accepted, when importing certificates from an external certificate authority. This can affect the behavior of the **crypto pki authenticate** and **crypto pki import pem** commands.

Use the **no** variant of this command to remove the specified fingerprint from the pre-accepted list.

Syntax

```
fingerprint <word>
no fingerprint <word>
```

Parameter	Description
<word>	The fingerprint as a series of 40 hexadecimal characters, optionally separated into multiple character strings.

Default By default, no fingerprints are pre-accepted for the trustpoint.

Mode Trustpoint Configuration

Usage notes Specifying a fingerprint adds it to a list of pre-accepted fingerprints for the trustpoint. When a certificate is imported, if it matches any of the pre-accepted values, then it will be saved in the system automatically. If the imported certificate's fingerprint does not match any pre-accepted value, then the user will be prompted to verify the certificate contents and fingerprint visually.

This command is useful when certificates from an external certificate authority are being transmitted over an insecure channel. If the certificate fingerprint is delivered via a separate messaging channel, then pre-entering the fingerprint value via cut-and-paste may be less errorprone than attempting to verify the fingerprint value visually.

The fingerprint is a series of 40 hexadecimal characters. It may be entered as a continuous string, or as a series of up to multiple strings separated by spaces. The input format is flexible because different certificate authorities may provide the fingerprint string in different formats.

Example To configure a fingerprint "5A81D34C 759CC4DA CFCA9F65 0303AD83 410B03AF" for the trustpoint named "example", use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# fingerprint 5A81D34C 759CC4DA CFCA9F65
0303AD83 410B03AF
```

Related commands crypto pki authenticate

crypto pki import pem

no crypto pki certificate

Overview Use this command to delete a certificate with the specified fingerprint from the specified trustpoint.

Syntax

```
no crypto pki certificate <trustpoint> <word>
```

Parameter	Description
<trustpoint>	The name of the trustpoint.
<word>	The fingerprint as a series of 40 hexadecimal characters, optionally separated into multiple character strings.

Default By default, no fingerprints are pre-accepted for the trustpoint.

Mode Privileged Exec

Usage notes The fingerprint can be found in the output of the **show crypto pki certificates** command. If there are dependent certificates in the trustpoint (i.e., if other certificates were signed by the specified certificate), the command will be rejected.

If the specified certificate is the root CA certificate and the trustpoint represents a locally selfsigned CA, then the corresponding private key is also deleted from the system. Deleting the root CA certificate effectively resets the trustpoint to an unauthenticated state.

Example To delete a certificate with the fingerprint "594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792" from the trustpoint “example”, use the following commands:

```
awplus> enable
awplus# no crypto pki certificate example
594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792
```

Related commands no crypto pki trustpoint

show crypto pki certificates

rsakeypair (ca-trustpoint)

Overview Use this command to declare which RSA key pair should be used to enroll the local server with the trustpoint. Note that this defines the key pair used with the server certificate, not the key pair used with the root CA certificate.

Use the **no** variant of this command to restore the default value, “server-default”.

Syntax

```
rsakeypair <keylabel> [<1024-4096>]
no rsakeypair
```

Parameter	Description
<keylabel>	The key to be used with the server certificate for this trustpoint. The name must start with an alphanumeric character, and may only contain alphanumeric characters, underscores, dashes, or periods. The maximum length of the name is 63 characters.
<1024-4096>	The bit length for the key, to be used if the key is implicitly generated during server enrollment.

Default The default value for **keylabel** is “server-default”.

The default value for the key bit length is 2048.

Mode Trustpoint Configuration

Usage notes If the label specified does not refer to an existing key created by the **crypto key generate rsa** command, the key will be implicitly generated when the **crypto pki enroll** command is issued to generate the server certificate or the server certificate signing request. The optional numeric parameter defines the bit length for the key, and is only applicable for keys that are implicitly created during enrollment.

This command does not affect server certificates or server certificate signing requests that have already been generated. The trustpoint’s server certificate is set to use whatever key pair was specified for the trustpoint at the time the **crypto pki enroll** command is issued.

The default key pair is “server-default”. The default bit length is 2048 bits.

Example To configure trustpoint "example" to use the key pair "example-server-key" with a bit length of 2048, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# rsakeypair example-server-key 2048
```

Related commands crypto key generate rsa

show crypto key mypubkey rsa

Overview Use this command to display information about the specified Rivest-Shamir-Adleman encryption key.

Syntax

```
show crypto key mypubkey rsa [<keylabel>]
```

Parameter	Description
<keylabel>	The name of the key to be shown, if specified.

Default By default, all keys will be shown.

Mode Privileged Exec

Usage notes If no key label is specified, information about all keys is shown. The command displays the bit length of the key, a key fingerprint (a hash of the key contents to help uniquely identify a key), and a list of trustpoints in which the server certificate is using the key.

The specified keys must exist.

Example To show all keys, use the following commands:

```
awplus> enable
awplus# show crypto key mypubkey rsa
```

Output Figure 19-1: Example output from **show crypto key mypubkey rsa**

```
awplus#show crypto key mypubkey rsa
--------------------
RSA Key Pair "example-server-key":
   Key size    : 2048 bits
   Fingerprint : 1A605D73 C2274CB7 853886B3 1C802FC6 7CDE45FB
   Trustpoints : example
--------------------
RSA Key Pair "server-default":
   Key size    : 2048 bits
   Fingerprint : 34AC4D2D 5249A168 29D426A3 434FFC59 C4A19901
   Trustpoints : local
```

Related commands crypto key generate rsa

show crypto pki certificates

Overview Use this command to display information about existing certificates for the specified trustpoint.

Syntax

```
show crypto pki certificates [<trustpoint>]
```

Parameter	Description
<trustpoint>	The trustpoint for which the certificates are to be shown.

Default By default, the certificates for all trustpoints are shown.

Mode Privileged Exec

Usage notes If no trustpoint is specified, certificates for all trustpoints are shown. The command displays the certificates organized into certificate chains. It starts with the server certificate and then displays its issuer, and continues up the issuer chain until the root CA certificate is reached.

For each certificate, the command displays the certificate type, the subject's distinguished name (the entity identified by the certificate), the issuer's distinguished name (the entity that signed the certificate), the validity dates for the certificate, and the fingerprint of the certificate. The fingerprint is a cryptographic hash of the certificate contents that uniquely identifies the certificate.

The specified trustpoints must already exist.

Example To show the certificates for the trustpoint "example", use the following command:

```
awplus> enable
awplus# show crypto pki certificates example
```

Output Figure 19-2: Example output from **show crypto pki certificates**

```
awplus>enable
awplus#show crypto pki certificates example
--------------------
Trustpoint "example" Certificate Chain
--------------------
Server certificate
   Subject     : /O=local/CN=local.loc.lc
   Issuer      : /C=NZ/CN=local_Signing_CA
   Valid From  : Nov 11 15:35:21 2015 GMT
   Valid To    : Aug 31 15:35:21 2018 GMT
   Fingerprint : 5A81D34C 759CC4DA CFCA9F65 0303AD83 410B03AF
Intermediate CA certificate
   Subject     : /C=NZ/CN=example_Signing_CA
   Issuer      : /C=NZ/CN=example_Root_CA
   Valid From  : Sep 3 18:45:01 2015 GMT
   Valid To    : Oct 10 18:45:01 2020 GMT
   Fingerprint : AE2D5850 9867D258 ABBEE95E 2E0E3D81 60714920
Imported root certificate
   Subject     : /C=NZ/CN=example_Root_CA
   Issuer      : /C=NZ/CN=example_Root_CA
   Valid From  : Jul 23 18:12:10 2015 GMT
   Valid To    : May 12 18:12:10 2025 GMT
   Fingerprint : 594EDEF9 C7C4308C 36D408E0 77E784F0 A59E8792
```

Related commands crypto pki trustpoint

show crypto pki enrollment user

Overview Use this command to display a list of trustpoints for which RADIUS user enrollments have been performed, using the **crypto pki enroll user** command. This indicates that PKCS#12 files for the user are available for export for the given trustpoints, using the **crypto pki export pkcs12** command.

Syntax

```
crypto pki enrollment user <username>
```

Parameter	Description
<username>	The user for which enrollments are to be shown.

Mode Privileged Exec

Example To show the list of trustpoints to which user "exampleuser1" is enrolled, use the following commands:

```
awplus> enable
awplus(config)# show crypto pki enrollment user exampleuser1
```

Output Figure 19-3: Example output from **show crypto pki enrollment user**

```
awplus> enable
awplus# show crypto pki enrollment user exampleuser1
User "exampleuser1" is enrolled to the following trustpoints:
local,example
```

Related commands

crypto pki enroll user

crypto pki export pkcs12

show crypto pki trustpoint

Overview Use this command to display information about the specified trustpoint.

Syntax

```
show crypto pki trustpoint [<trustpoint>]
```

Parameter	Description
<trustpoint>	The name of the trustpoint to be shown

Default By default, all trustpoints are shown.

Mode Privileged Exec

Usage notes If no trustpoint is specified, information about all trustpoints is shown. The command displays the authentication status of the trustpoint, the fingerprint of the root CA certificate (if it exists), the enrollment status of the local server with the trustpoint, a list of any applications that are configured to use the trustpoint, and the trustpoint parameters that were configured from trustpoint-configuration mode.

The specified trustpoints must already exist.

Example To show the details of the trustpoint “example”, use the following commands:

```
awplus> enable
awplus# show crypto pki trustpoint example
```

Output Figure 19-4: Example output from **show crypto pki trustpoint**

```
awplus> enable
awplus# show crypto pki trustpoint example
--------------------
Trustpoint "example"
   Type             : Self-signed certificate authority
   Root Certificate: 50C1856B EEC7555A 0F3A61F6 690D9463 67DF74D1
   Local Server     : The server is enrolled to this trustpoint.
   Server Key       : example-server-key
   Applications     : RADIUS

Authentication and Enrollment Parameters:
   Enrollment       : selfsigned
   RSA Key Pair     : example-server-key (2048 bits)
--------------------
```

Related commands

crypto pki trustpoint

show crypto pki certificates

show hash

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

Syntax

```
show hash <filename>
```

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

Mode Privileged Exec

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

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

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

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

Output Figure 19-5: Example output from **show hash**

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

Command changes Version 5.5.3-0.1: command added

subject-name (ca-trustpoint)

Overview Use this command to specify the distinguished name string that should be used for the subject field in the server certificate, when enrolling the server (generating the server certificate or server certificate signing request).

Syntax

```
subject-name <word>
```

Parameter	Description
<word>	Specify the subject name as a distinguished name string. Complex strings (e.g., strings containing spaces) should be surrounded with double-quote characters.

Default If no subject name is specified for the trustpoint, then the system automatically builds a name of the form "/O=AlliedWare Plus/CN=xxxx.yyyy.zzz", where "xxxx" is the hostname of the system and "yyyy.zzz" is the default search domain for the system.

Mode Trustpoint Configuration

Usage notes The subject name is specified as a variable number of fields, where each field begins with a forward-slash character ("/"). Each field is of the form "XX=value", where "XX" is the abbreviation of the node type in the tree.

Common values include:

- "C" (country),
- "ST" (state),
- "L" (locality),
- "O" (organization),
- "OU" (organizational unit), and
- "CN" (common name).

Of these fields, "CN" is usually the most important.

NOTE: *For a server certificate, many applications require that the network name of the server matches the common name in the server's certificate.*

Example To configure the trustpoint named "example" and set its subject name, use the following commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto pki trustpoint example
awplus(ca-trustpoint)# subject-name "/O=My
Company/CN=192.168.1.1
```

Related commands crypto pki enroll

20 TACACS+ Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure the device to use TACACS+ servers. For more information about TACACS+, see the TACACS+ Feature Overview and Configuration Guide.

Command List

- "aaa authorization commands" on page 543
- "aaa authorization config-commands" on page 545
- "authorization commands" on page 546
- "ip tacacs source-interface" on page 548
- "show tacacs+" on page 549
- "tacacs-server host" on page 551
- "tacacs-server key" on page 553
- "tacacs-server timeout" on page 554

aaa authorization commands

Overview This command configures a method list for commands authorization that can be applied to console or VTY lines. When command authorization is enabled for a privilege level, only authorized users can executed commands in that privilege level.

Use the **no** variant of this command to remove a named method list or disable the default method list for a privilege level.

Syntax

```
aaa authorization commands <privilege-level>
{default|<list-name>} group tacacs+ [none]
```

```
no aaa authorization commands <privilege-level>
{default|<list-name>}
```

Parameter	Description
<privilege-level>	The privilege level of the set of commands the method list will be applied to. AlliedWare Plus defines three sets of commands, that are indexed by a level value: **Level = 1**: All commands that can be accessed by a user with privilege level between 1 and 6 inclusive **Level = 7:** All commands that can be accessed by a user with privilege level between 7 and 14 inclusive **Level = 15**: All commands that can be accessed by a user with privilege level 15
`group`	Specify the server group where authorization messages are sent. Only the `tacacs+` group is available for this command.
`tacacs+`	Use all TACACS+ servers configured by the tacacs-server host command.
`default`	Configure the default authorization commands method list.
<list-name>	Configure a named authorization commands method list
`none`	If specified, this provides a local fallback to command authorization so that if authorization servers become unavailable then the device will accept all commands normally allowed for the privilege level of the user.

Mode Global Configuration

Usage notes TACACS+ command authorization provides centralized control of the commands available to a user of an AlliedWare Plus device. Once enabled:

- The command string and username are encrypted and sent to the first available configured TACACS+ server (the first server configured) for authorization.

- The TACACS+ server decides if the user is authorized to execute the command and returns the decision to the AlliedWare Plus device.
- Depending on this decision the device will then either execute the command or notify the user that authorization has failed.

If multiple TACACS+ servers are configured, and the first server is unreachable or does not respond, the other servers will be queried, in turn, for an authorization decision. If all servers are unreachable and a local fallback has been configured, with the **none** parameter, then commands are authorized based on the user's privilege level; the same behavior as if command authorization had not been configured. If, however, the local fallback is not configured and all servers become unreachable then all commands except **logout**, **exit**, and **quit** will be denied.

The **default** method list is defined with a local fallback unless configured differently using this command.

Example To configure a commands authorization method list, named TAC15, using all TACACS+ servers to authorize commands for privilege level 15, with a local fallback, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authorization commands 15 TAC15 group tacacs+ none
```

To configure the default method list to authorize commands for privilege level 7, with no local fallback, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authorization commands 7 default group tacacs+
```

To remove the authorization method list TAC15, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authorization commands 15 TAC15
```

Related commands

aaa authorization config-commands

authorization commands

tacacs-server host

Command changes Version 5.4.6-2.1: command added

aaa authorization config-commands

Overview Use this command to enable command authorization on configuration mode commands. By default, command authorization applies to commands in exec mode only.

Use the **no** variant of this command to disable command authorization on configuration mode commands.

Syntax

```
aaa authorization config-commands
no aaa authorization config-commands
```

Default By default, command authorization is disabled on configuration mode commands.

Mode Global Configuration

Usage notes If authorization of configuration mode commands is not enabled then all configuration commands are accepted by default, including command authorization commands.

NOTE: *Authorization of configuration commands is required for a secure TACACS+ command authorization configuration as it prevents the feature from being disabled to gain access to unauthorized exec mode commands.*

Example To enable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authorization config-commands
```

To disable command authorization for configuration mode commands, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authorization config-commands
```

Related commands aaa authorization commands

authorization commands

tacacs-server host

Command changes Version 5.4.6-2.1: command added

authorization commands

Overview This command applies a command authorization method list, defined using the aaa authorization commands command, to console and VTY lines.

Use the **no** variant of this command to reset the command authorization configuration on the console and VTY lines.

Syntax

```
authorization commands <privilege-level> {default|<list-name>}
no authorization commands <privilege-level>
```

Parameter	Description
<privilege-level>	The privilege level of the set of commands the method list will be applied to. AlliedWare Plus defines three sets of commands, that are indexed by a level value: **Level = 1**: All commands that can be accessed by a user with privilege level between 1 and 6 inclusive **Level = 7:** All commands that can be accessed by a user with privilege level between 7 and 14 inclusive **Level = 15**: All commands that can be accessed by a user with privilege level 15
`default`	Configure the default authorization commands method list.
<list-name>	Configure a named authorization commands method list

Default The **default** method list is applied to each console and VTY line by default.

Mode Line Configuration

Usage notes If the specified method list does not exist users will not be enable to execute any commands in the specified method list on the specified VTY lines.

Example To apply the TAC15 command authorization method list with privilege level 15 to VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# authorization commands 15 TAC15
```

To reset the command authorization configuration with privilege level 15 on VTY lines 0 to 5, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# no authorization commands 15
```

Related commands aaa authorization commands

aaa authorization config-commands

tacacs-server host

Command changes Version 5.4.6-2.1: command added

ip tacacs source-interface

Overview This command sets the source interface, or IP address, to use for all TACACS+ packets sent from the device. By default, TACACS+ packets use the source IP address of the egress interface.

Use the **no** variant of this command to remove the source interface configuration and use the source IP address of the egress interface.

Syntax

```
ip tacacs source-interface {<interface>|<ip-address>}
no ip tacacs source-interface
```

Parameter	Description
<interface>	Interface name.
<ip-address>	IP address in the dotted decimal format A.B.C.D.

Default The source IP address of outgoing TACACS+ packets default to the IP address of the egress interface.

Mode Global Configuration

Usage notes Setting the source interface ensures that all TACACS+ packets sent from the device will have the same source IP address. Once configured this affects all TACACS+ packets, namely accounting, authentication, and authorization.

If the specified interface is down or there is no IP address on the interface, then the source IP address of outgoing TACACS+ packets will default to the IP address of the egress interface.

Example To configure all outgoing TACACS+ packets to use the IP address of the loop-back "lo" interface as the source IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ip tacacs source-interface lo
```

To reset the source interface configuration for all TACACS+ packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip tacacs source-interface
```

Related commands tacacs-server host

show tacacs+

Command changes Version 5.4.6-2.1: command added

show tacacs+

Overview This command displays the current TACACS+ server configuration and status.

Syntax

```
show tacacs+
```

Mode User Exec and Privileged Exec

Example To display the current status of TACACS+ servers, use the command:

```
awplus# show tacacs+
```

Output Figure 20-1: Example output from the **show tacacs+** command

```
TACACS+ Global Configuration
  Source Interface    : not configured
  Timeout             : 5 sec

Server Host/      Server
IP Address        Status
------------------------------------------------------------
192.168.1.10      Alive
192.168.1.11      Unknown
```

Table 1: Parameters in the output of the **show tacacs+** command

Output Parameter	Meaning	
`Source Interface`	IP address of source interface if set with ip tacacs source-interface.	
`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 unkown.
	`Unreachable`	The server is unreachable.
	`Unresolved`	The server name can not be resolved.

Command changes Version 5.4.6-2.1: **Source Interface** parameter added

tacacs-server host

Overview Use this command to specify a remote TACACS+ server host for authentication, authorization and accounting, and to set the shared secret key to use with the TACACS+ server. The parameters specified with this command override the corresponding global parameters for TACACS+ servers.

Use the **no** variant of this command to remove the specified server host as a TACACS+ authentication and authorization server.

Syntax

```
tacacs-server host {<host-name>|<ip-address>} [key [8]
<key-string>]
```

```
no tacacs-server host {<host-name>|<ip-address>}
```

Parameter	Description
<host-name>	Server host name. The DNS name of the TACACS+ server host.
<ip-address>	The IP address of the TACACS+ server host, in dotted decimal notation A.B.C.D.
`key`	Set shared secret key with TACACS+ servers.
`8`	Specifies that you are entering a password as a string that has already been encrypted instead of entering a plain text password. The running config displays the new password as an encrypted string even if password encryption is turned off.
<key-string>	Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and the TACACS+ server. This key must match the encryption used on the TACACS+ server. This setting overrides the global setting of the tacacs-server key command. If no key value is specified, the global value is used.

Default No TACACS+ server is configured by default.

Mode Global Configuration

Usage A TACACS+ server host cannot be configured multiple times like a RADIUS server.

As many as four TACACS+ servers can be configured and consulted for login authentication, enable password authentication and accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, not if a login authentication attempt is rejected. The reasons a server would fail are:

- it is not network reachable
- it is not currently TACACS+ capable

- it cannot communicate with the switch properly due to the switch and the server having different secret keys

Examples

To add the server tac1.company.com as the TACACS+ server host, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host tac1.company.com
```

To set the secret key to 'secret' on the TACACS+ server 192.168.1.1, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host 192.168.1.1 key secret
```

To remove the TACACS+ server tac1.company.com, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server host tac1.company.com
```

Related commands

aaa accounting commands

aaa authentication login

tacacs-server key

tacacs-server timeout

show tacacs+

Command changes

Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

tacacs-server key

Overview This command sets a global secret key for TACACS+ authentication, authorization and accounting. The shared secret text string is used for TACACS+ communications between the switch and all TACACS+ servers.

Note that if no secret key is explicitly specified for a TACACS+ server with the tacacs-server host command, the global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to remove the global secret key.

Syntax

```
tacacs-server key [8] <key-string>
no tacacs-server key
```

Parameter	Description
8	Specifies a string in an encrypted format instead of plain text. The running config will display the new password as an encrypted string even if password encryption is turned off.
<key-string>	Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and all TACACS+ servers. This key must match the encryption used on the TACACS+ server.

Mode Global Configuration

Usage notes Use this command to set the global secret key shared between this client and its TACACS+ servers. If no secret key is specified for a particular TACACS+ server using the tacacs-server host command, this global key is used.

Examples To set the global secret key to `secret` for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server key secret
```

To delete the global secret key for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server key
```

Related commands tacacs-server host

show tacacs+

tacacs-server timeout

Overview Use this command to specify the TACACS+ global timeout value. The timeout value is how long the device waits for a reply to a TACACS+ request before considering the server to be dead.

Note that this command configures the **timeout** parameter for TACACS+ servers globally.

The **no** variant of this command resets the transmit timeout to the default (5 seconds).

Syntax

```
tacacs-server timeout <seconds>
no tacacs-server timeout
```

Parameter	Description
<seconds>	TACACS+ server timeout in seconds, in the range 1 to 1000.

Default The default timeout value is 5 seconds.

Mode Global Configuration

Examples To set the timeout value to 3 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server timeout 3
```

To reset the timeout period for TACACS+ servers to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server timeout
```

Related commands tacacs-server host

show tacacs+

Part 5: Network Management

21 AMF and AMF Plus Commands

Introduction

Overview

This chapter provides an alphabetical reference for AMF and AMF Plus commands. AMF is the Allied Telesis Autonomous Management Framework™, and AMF Plus is an expanded version of AMF. Both AMF and AMF Plus are a suite of features that combine to simplify network management across all supported network equipment from the core to the edge. They also integrate with Vista Manager, our graphical monitoring and management platform.

On the AlliedWare Plus command line, AMF and AMF Plus are identical. The difference between them is in Vista Manager, where AMF Plus includes additional AMF Plus intent-based networking features.

In the rest of this chapter, we use 'AMF' to refer to both AMF and AMF Plus.

AMF master nodes

Every AMF network must have at least one master node, which acts as the core of the AMF network. Not all AlliedWare Plus devices are capable of acting as a AMF master. See the AMF Feature Overview and Configuration Guide for information about master support.

AMF edge

AlliedWare Plus CentreCOM® Series switches can only be used as edge switches in an AMF network. The full management power and convenience of AMF is available on these switches, but they can only link to one other AMF node. They cannot form cross-links or virtual links.

AMF naming convention

When AMF is enabled on a device, it will automatically be assigned a host name. If a host name has already been assigned, by using the command hostname on page 171, this will remain. If however, no host name has been assigned, then the name applied will be the prefix, **host_** followed (without a space) by the MAC address of the device. For example, a device whose MAC address is **0016.76b1.7a5e** will have the name **host_0016_76b1_7a5e** assigned to it.

To efficiently manage your network using AMF, we strongly advise that you devise a naming convention for your network devices, and apply an appropriate hostname to each device in your AMF network.

AMF and STP

On AR-Series UTM firewalls and Secure VPN routers, you cannot use STP at the same time as AMF.

Command List

- "application-proxy ip-filter" on page 562
- "application-proxy quarantine-vlan" on page 563
- "application-proxy redirect-url" on page 564
- "application-proxy threat-protection" on page 565
- "application-proxy threat-protection send-summary" on page 567
- "application-proxy whitelist advertised-address" on page 568
- "application-proxy whitelist enable" on page 569
- "application-proxy whitelist protection tls" on page 570
- "application-proxy whitelist server" on page 571
- "application-proxy whitelist trustpoint (deprecated)" on page 573
- "area-link" on page 574
- "atmf-arealink" on page 576
- "atmf-link" on page 578
- "atmf amfplus-license-only" on page 579
- "atmf area" on page 581
- "atmf area password" on page 583
- "atmf authorize" on page 585
- "atmf authorize provision" on page 587
- "atmf backup" on page 589
- "atmf backup area-masters delete" on page 590
- "atmf backup area-masters enable" on page 591
- "atmf backup area-masters now" on page 592
- "atmf backup area-masters synchronize" on page 593
- "atmf backup bandwidth" on page 594
- "atmf backup delete" on page 595
- "atmf backup enable" on page 596
- "atmf backup guests delete" on page 597
- "atmf backup guests enable" on page 598
- "atmf backup guests now" on page 599
- "atmf backup guests synchronize" on page 600
- "atmf backup now" on page 601
- "atmf backup redundancy enable" on page 603
- "atmf backup server" on page 604

- "atmf backup stop" on page 605
- "atmf backup synchronize" on page 606
- "atmf cleanup" on page 607
- "atmf container" on page 608
- "atmf container login" on page 609
- "atmf controller" on page 610
- "atmf distribute firmware" on page 611
- "atmf domain vlan" on page 613
- "atmf enable" on page 616
- "atmf group (membership)" on page 617
- "atmf guest-class" on page 619
- "atmf log-verbose" on page 621
- "atmf management subnet" on page 622
- "atmf management vlan" on page 625
- "atmf master" on page 627
- "atmf mtu" on page 628
- "atmf network-name" on page 629
- "atmf provision (interface)" on page 630
- "atmf provision node" on page 631
- "atmf reboot-rolling" on page 633
- "atmf recover" on page 637
- "atmf recover guest" on page 639
- "atmf recover led-off" on page 640
- "atmf recover over-eth" on page 641
- "atmf recovery-server" on page 642
- "atmf remote-login" on page 644
- "atmf restricted-login" on page 646
- "atmf retry guest-link" on page 648
- "atmf secure-mode" on page 649
- "atmf secure-mode certificate expire" on page 651
- "atmf secure-mode certificate expiry" on page 652
- "atmf secure-mode certificate renew" on page 653
- "atmf secure-mode enable-all" on page 654
- "atmf select-area" on page 656
- "atmf topology-gui enable" on page 657

- "atmf trustpoint" on page 658
- "atmf virtual-crosslink" on page 660
- "atmf virtual-link" on page 662
- "atmf virtual-link description" on page 665
- "atmf virtual-link protection" on page 666
- "atmf working-set" on page 668
- "bridge-group (amf-container)" on page 670
- "clear application-proxy threat-protection" on page 672
- "clear atmf links" on page 673
- "clear atmf links virtual" on page 674
- "clear atmf links statistics" on page 675
- "clear atmf recovery-file" on page 676
- "clear atmf secure-mode certificates" on page 677
- "clear atmf secure-mode statistics" on page 678
- "clone (amf-provision)" on page 679
- "configure boot config (amf-provision)" on page 681
- "configure boot system (amf-provision)" on page 683
- "copy (amf-provision)" on page 685
- "create (amf-provision)" on page 686
- "debug atmf" on page 688
- "debug atmf packet" on page 690
- "delete (amf-provision)" on page 692
- "discovery" on page 694
- "description (amf-container)" on page 696
- "erase factory-default" on page 697
- "firmware-url" on page 698
- "http-enable" on page 700
- "identity (amf-provision)" on page 702
- "license-cert (amf-provision)" on page 704
- "locate (amf-provision)" on page 706
- "log event-host" on page 708
- "login-fallback enable" on page 709
- "modeltype" on page 710
- "service atmf-application-proxy" on page 711
- "show application-proxy threat-protection" on page 712

- "show application-proxy whitelist advertised-address" on page 714
- "show application-proxy whitelist interface" on page 715
- "show application-proxy whitelist server" on page 717
- "show application-proxy whitelist supplicant" on page 718
- "show atmf" on page 720
- "show atmf area" on page 724
- "show atmf area guests" on page 727
- "show atmf area guests-detail" on page 729
- "show atmf area nodes" on page 731
- "show atmf area nodes-detail" on page 733
- "show atmf area summary" on page 735
- "show atmf authorization" on page 736
- "show atmf backup" on page 739
- "show atmf backup area" on page 743
- "show atmf backup guest" on page 745
- "show atmf container" on page 747
- "show atmf detail" on page 750
- "show atmf group" on page 752
- "show atmf group members" on page 754
- "show atmf guests" on page 756
- "show atmf guests detail" on page 758
- "show atmf links" on page 761
- "show atmf links detail" on page 763
- "show atmf links guest" on page 772
- "show atmf links guest detail" on page 774
- "show atmf links statistics" on page 778
- "show atmf nodes" on page 781
- "show atmf provision nodes" on page 783
- "show atmf recovery-file" on page 785
- "show atmf secure-mode" on page 786
- "show atmf secure-mode audit" on page 788
- "show atmf secure-mode audit link" on page 789
- "show atmf secure-mode certificates" on page 790
- "show atmf secure-mode sa" on page 793
- "show atmf secure-mode statistics" on page 796

- "show atmf tech" on page 798
- "show atmf virtual-links" on page 801
- "show atmf working-set" on page 803
- "show debugging atmf" on page 804
- "show debugging atmf packet" on page 805
- "show running-config atmf" on page 806
- "state" on page 807
- "switchport atmf-agentlink" on page 809
- "switchport atmf-arealink" on page 810
- "switchport atmf-crosslink" on page 812
- "switchport atmf-guestlink" on page 814
- "switchport atmf-link" on page 816
- "type atmf guest" on page 817
- "type atmf node" on page 818
- "undebug atmf" on page 820
- "username (atmf-guest)" on page 821

application-proxy ip-filter

Overview Use this command to enable global IP filtering on a device. Once enabled the device will add a global ACL in response to a threat message from an AMF Security (AMF-Sec) Controller.

Use the **no** variant of this command to disable global IP filtering.

Syntax

```
application-proxy ip-filter
no application-proxy ip-filter
```

Default Global IP filtering is disabled by default.

Mode Global Configuration

Usage notes For this feature to work, the AMF Application Proxy service needs to be enabled on your network, using the command service atmf-application-proxy.

Example To enable global IP filtering, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy ip-filter
```

To disable global IP filtering, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy ip-filter
```

Related commands

application-proxy redirect-url

application-proxy threat-protection

clear application-proxy threat-protection

service atmf-application-proxy

show application-proxy threat-protection

Command changes Version 5.4.7-2.5: command added

application-proxy quarantine-vlan

Overview Use this command to set the quarantine VLAN to use when an AMF Security (AMF-Sec) Controller detects a threat. The port/s on which the threat is detected are moved to this VLAN if the application-proxy threat-protection action is set to **quarantine**.

Use the **no** variant of this command to delete the quarantine VLAN. If no quarantine VLAN is specified then no quarantine action will be performed.

Syntax

```
application-proxy quarantine-vlan <vlan-id>
no application-proxy quarantine-vlan
```

Parameter	Description
<vlan-id>	The ID of the VLAN to use. In the range 1-4094.

Default By default, no quarantine VLAN is configured.

Mode Global Configuration

Example To configure VLAN 100 as the quarantine VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy quarantine-vlan 100
```

To delete the quarantine VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy quarantine-vlan
```

Related commands

application-proxy threat-protection

clear application-proxy threat-protection

application-proxy threat-protection send-summary

service atmf-application-proxy

show application-proxy threat-protection

Command changes Version 5.4.7-2.2: command added

application-proxy redirect-url

Overview Use this command to redirect a user to a helpful URL when they are blocked because of an application-proxy ip-filter.

Use the **no** variant of this command to remove the URL redirect.

Syntax

```
application-proxy redirect-url <url>
no application-proxy redirect-url
```

Parameter	Description
<url>	URL to redirect the user to.

Default No URL is configured by default.

Mode Global Configuration

Example To configure a redirect URL, use the command:

```
awplus# application-proxy redirect-url http://my.dom/help.html
```

To remove a redirect URL, use the command:

```
awplus# no application-proxy redirect-url
```

Related commands

application-proxy ip-filter

application-proxy threat-protection

clear application-proxy threat-protection

service atmf-application-proxy

show application-proxy threat-protection

Command changes Version 5.4.9-0.1: command added

application-proxy threat-protection

Overview Use this command to set the blocking action to take when a threat detected message is received from an AMF Security (AMF-Sec) Controller.

Use the **no** variant of this command to disable threat protection blocking actions on the port.

Syntax

```
application-proxy threat-protection
{drop|link-down|quarantine|log-only}
```

```
no application-proxy threat-protection
```

Parameter	Description
`drop`	Drop the traffic that generates the threat reports. This is a Layer 2 drop. Note that the device will only drop packets that arrive at the port, not packets sent from the port.
`link-down`	Take the link down in response to threats, by setting it to error disabled.
`quarantine`	Move the offending port to a quarantine VLAN.
`log-only`	Log when a threat is detected.

Default Threat protection is disabled by default.

Mode Interface Configuration

Example To set the threat protection blocking action on port1.0.4 to drop, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# application-proxy threat-protection drop
```

To disable threat protection blocking actions on port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no application-proxy threat-protection
```

Related commands

application-proxy quarantine-vlan

application-proxy threat-protection send-summary

clear application-proxy threat-protection

service atmf-application-proxy

show application-proxy threat-protection

Command changes

Version 5.5.2-0.1: added to switch ports on AR series devices

Version 5.4.9-0.1: **log-only** parameter added

Version 5.4.7-2.2: command added

application-proxy threat-protection send-summary

Overview Use this command to send a summary of all current threat-protection blocking requests to all AMF Application Proxy service nodes. This command can only be performed on an AMF master.

Syntax
```
application-proxy threat-protection send-summary
```

Mode Privileged Exec

Example To send a summary of all current threat-protection blocking requests to all AMF Application Proxy service nodes, use the command:

```
awplus# application-proxy threat-protection send-summary
```

Related commands
- application-proxy quarantine-vlan
- application-proxy threat-protection
- clear application-proxy threat-protection
- service atmf-application-proxy
- show application-proxy threat-protection

Command changes Version 5.4.7-2.2: command added

application-proxy whitelist advertised-address

Overview Use this command to register a Layer 3 interface, and the IPv4 address that is attached to this interface, as the advertised application-proxy whitelist address for a device.

Use the **no** variant of this command to stop advertising the Layer 3 interface and its associated IPv4 address.

Syntax

```
application-proxy whitelist advertised-address <interface>
no application-proxy whitelist advertised-address
```

Parameter	Description
<interface>	Layer 3 interface to configure as the advertised address.

Default No address advertised by default.

Mode Global Configuration

Example To configure the IPv4 address attached to VLAN 1as the advertised address, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist advertised-address
vlan1
```

To remove the advertised address, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy whitelist
advertised-address
```

Related commands application-proxy whitelist server

show application-proxy whitelist advertised-address

Command changes Version 5.4.9-1.1: command added

application-proxy whitelist enable

Overview Use this command to enable application-proxy whitelist based authentication on an interface.

Use the **no** variant of this command to disable the whitelist authentication.

Syntax

```
application-proxy whitelist enable
no application-proxy whitelist enable
```

Default Application-proxy whitelist is disabled by default.

Mode Interface Configuration

Usage notes When **port-control** is set to **auto**, the 802.1X authentication feature is executed on the interface, but only if the **aaa authentication dot1x** command has been issued.

If you attempt to change the authentication configuration on an interface that has threat protection quarantine configured, you will see the following error message:

```
% portx.x.x: Application Proxy quarantine configuration must be
removed before port authentication is changed
```

Before changing the interface's authentication configuration you must either:

- remove the interface's threat protection configuration, or
- shut down the interface.

Example To enable application-proxy whitelist authentication on the interface port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# application-proxy whitelist enable
```

To disable application-proxy whitelist authentication on the interface port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no application-proxy whitelist enable
```

Related commands

application-proxy whitelist server

show application-proxy whitelist interface

show application-proxy whitelist server

show application-proxy whitelist supplicant

Command changes Version 5.4.9-0.1: command added

application-proxy whitelist protection tls

Overview Use this command to configure the application-proxy whitelist control channel to use TLS protection. If no trustpoint is specified then TLS will operate without authentication.

Use the **no** variant of this command to stop using TLS.

Syntax

```
application-proxy whitelist protection tls [trustpoint <name>]
no application-proxy whitelist protection tls
```

Parameter	Description
`trustpoint`	Specify an optional trustpoint. If no trustpoint is specified then TLS will operate without authentication.
<name>	Name of the trustpoint.

Default TLS is disabled by default.

Mode Global Configuration

Example To configure an AMF application-proxy whitelist to use TLS with the trustpoint 'corpca', use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist protection tls
trustpoint corpca
```

To configure an AMF application-proxy whitelist to stop using TLS, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy whitelist protection tls
```

Related commands

application-proxy whitelist enable

application-proxy whitelist server

show application-proxy whitelist server

Command changes Version 5.5.0-2.1: command added

application-proxy whitelist server

Overview Use this command to set an AMF master to act as a whitelist authentication proxy between AMF members, acting as Network Access Servers, and an external whitelist RADIUS server.

Use the **no** variant of this command to disable the whitelist proxy functionality.

Syntax

```
application-proxy whitelist server <ip-address> key <key>
[auth-port <1-65535>]
```

```
no application-proxy whitelist server
```

Parameter	Description
<ip-address>	IPv4 address of the upstream RADIUS server in dotted decimal format A.B.C.D.
`key` *<key>*	Set the shared secret encryption key for communication with the upstream RADIUS server.
`auth-port` *<1-65535>*	Set the RADIUS server UDP port. This is only necessary if you don't want to use the default port 1812.

Default Disabled by default.

Mode Global Configuration

Example To configure an AMF master to work as a proxy to the external RADIUS server 192.168.1.10, with shared secret 'mysecurekey', on port 1822, use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist server 192.168.1.10
key mysecurekey auth-port 1822
```

To configure an AMF master to work as a proxy to the external RADIUS server 192.168.1.10, with shared secret 'mysecurekey', on the default port (1812), use the commands:

```
awplus# configure terminal
awplus(config)# application-proxy whitelist server 192.168.1.10
key mysecurekey
```

To disable the whitelist proxy, use the commands:

```
awplus# configure terminal
awplus(config)# no application-proxy whitelist server
```

Related commands

application-proxy whitelist enable

service atmf-application-proxy

show application-proxy whitelist interface

show application-proxy whitelist server

show application-proxy whitelist supplicant

Command changes Version 5.4.9-0.1: command added

application-proxy whitelist trustpoint (deprecated)

Overview This command has been deprecated. It has been replaced by the application-proxy whitelist protection tls command.

This command sets the trustpoint to use when communicating with the external whitelist RADIUS server. This enables RADIUS over TLS (RadSec) protection.

Syntax

```
application-proxy whitelist trustpoint <name>
no application-proxy whitelist trustpoint
```

Command changes Version 5.4.9-1.1: command added

Version 5.5.0-2.1: command deprecated

area-link

Overview Use this command to create an area-link between a Virtual AMF Appliance (VAA) host controller and an AMF container.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the AMF Feature Overview and Configuration Guide for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove an area-link from a container.

Syntax

```
area-link <area-name>
no area-link
```

Parameter	Description
<area-name>	AMF area name of the container's area.

Mode AMF Container Configuration

Usage notes The AMF area-link connects the AMF controller on a VAA host to the AMF container. Once a container has been created with the atmf container command and an area-link configured with the **area-link** command, it can be enabled using the state command.

You can only configure a single area-link on a container. You will see the following message if you try and configure a second one:

```
% AreaLink already configured for this container
```

Each container has two virtual interfaces:

- Interface eth0, used to connect to the AMF controller on the VAA host via an AMF area-link, configured using this area-link command.
- Interface eth1, used to connect to the outside world using a bridged L2 network link, configured using the bridge-group (amf-container) command.

See the AMF Feature Overview and Configuration_Guide for more information on these virtual interfaces and links.

Example To create the area-link to "wlg" on container "vac-wlg-1", use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# area-link wlg
```

To remove an area-link from container “vac-wlg-1”, use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# no area-link
```

Related commands

atmf container

show atmf container

Command changes

Version 5.4.7-0.1: command added

atmf-arealink

Overview This command to enable an Eth interface, on an AR-series device, as an AMF area link. AMF area links are designed to operate between two nodes in different areas in an AMF network. This command is only available if your network is running in AMF secure mode (see atmf secure-mode for more information on AMF secure mode).

Use the **no** variant of this command to remove any AMF area links that may exist for the selected Eth interface.

Syntax

```
atmf-arealink remote-area <area-name> vlan <2-4094>
no atmf-arealink
```

Parameter	Description
<area-name>	The name of the remote area that the interface is connecting to.
<2-4094>	The VLAN ID for the link. This VLAN cannot be used for any other purpose, and the same VLAN ID must be used at each end of the link.

Default By default, no area links are configured

Mode Eth interface on an AR-series device.

Usage notes Run this command on the interface at both ends of the link.

Each area must have the area-name configured, and the same area password must exist on both ends of the link.

Running this command will synchronize the area information stored on the two nodes.

You can configure multiple area links between two area nodes, but only one area link at any time will be in use. All other area links will block information, to prevent network storms.

NOTE: *See the switchport atmf-arealink command to configure an AMF area link on an a switch port or link aggregator*

Example To configure eth1 as an AMF area link to the 'Auckland' area on VLAN 6, use the following commands:

```
master_1# configure terminal
master_1(config)# interface eth1
master_1(config-if)# atmf-arealink remote-area Auckland vlan 6
```

To remove eth1 as an AMF area link, use the following commands:

```
master_1# configure terminal
master_1(config)# interface eth1
master_1(config-if)# no atmf-arealink
```

Related commands

atmf area

atmf area password

atmf virtual-link

show atmf links

Command changes

Version 5.5.0-1.1: command added

atmf-link

Overview Use this command to enable an Eth interface on an AR-series device as an up/down AMF link. This command is only available if your network is running in AMF secure mode (see atmf secure-mode for more information on AMF secure mode).

Use the **no** variant of this command to remove any AMF link that may exist for the selected Eth interface.

Syntax

```
atmf-link
no atmf-link
```

Mode Eth interface on an AR-series device.

Usage notes Up/down links and virtual links interconnect domains in a vertical hierarchy, with the highest domain being the core domain. In effect, they form a tree of interconnected AMF domains. This tree must be loop-free. Therefore you must configure your up/down and virtual links so that no loops are formed.

If you run the command and AMF secure mode is not enabled, you will see the following error message:

```
Node_1(config)#int eth1
Node_1(config-if)#atmf-link
% Cannot configure eth1 because atmf secure-mode is not enabled.
```

NOTE: *See the switchport atmf-link command to configure an AMF up/down link on an a switch port or link aggregator*

Example To configure eth1 as an AMF up/down link, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface eth1
Node_1(config-if)# atmf-link
```

To remove eth1 as an AMF up/down link, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface eth1
Node_1(config-if)# no atmf-link
```

Related commands

atmf recover over-eth

atmf secure-mode

show atmf detail

show atmf links

switchport atmf-link

Command changes Version 5.5.0-1.1: command added

atmf amfplus-license-only

Overview Use this command if you want to use the AMF Plus features in Vista Manager EX, and you have a mixture of AMF and AMF Plus licenses on your master node. This command sets the AMF network to only count **AMF Plus** licensed nodes.

Use the **no** variant of this command to include both AMF and AMF Plus licenses when calculating the number of licensed nodes in an area count.

Syntax

```
atmf amfplus-license-only
no atmf amfplus-license-only
```

Default The **no** version is the default. That is, consider both AMF and AMF Plus licenses when calculating the number of licensed nodes.

Mode Global Configuration

Usage notes From software version 5.5.2-2.3 onwards, AMF licenses are no longer available to purchase. Instead, AMF Plus licenses become available. Existing AMF licenses remain valid. You only need to change to AMF Plus licenses if you want to manage more nodes, or use the new AMF Plus menu in Vista Manager.

CAUTION: *If the network has more AMF nodes than are licensed with AMF Plus:*

- AMF Plus will still be enabled in Vista Manager EX (provided there is no AMF license)
- any AMF nodes above the license count won't join the AMF network.

The AMF Plus menu replaces the AOI menu in Vista Manager EX when all the AMF Masters and Controllers have:

- An AMF Plus Controller/Master license on all Masters and Controllers, and
- No AMF Controller/Master licenses applied, or AMF Controller/Master licenses disabled with this command.

Example To set the AMF network to only count AMF Plus licensed nodes, use the commands:

```
awplus#configure terminal
awplus(config)#atmf amfplus-license-only
```

Output Figure 21-1: Example using **atmf amfplus-license-only**

```
ATMF Summary Information:
ATMF Status           : Enabled
Network Name          : gtnet
Node Name             : node2
Role                  : Master
Restricted login      : Enabled
Secure Mode           : Disabled
Current ATMF Guests   : 0
Current ATMF Nodes    : 10
Total number of licensed nodes available is 22

node2#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
node2(config)#atmf amfplus-license-only
node2(config)#15:41:36 node2 ATMF[1041]: The number of nodes
allowed on this ATMF network is 12

node2(config)#do show atmf
ATMF Summary Information:

ATMF Status           : Enabled
Network Name          : gtnet
Node Name             : node2
Role                  : Master
Restricted login      : Enabled
Secure Mode           : Disabled
Current ATMF Guests   : 0
Current ATMF Nodes    : 10
Master is configured to allow only AMFPLUS Licenses
Total number of licensed nodes available is 12
```

Related commands show atmf

Command changes Version 5.5.3-0.1: command added

atmf area

Overview This command creates an AMF area and gives it a name and ID number.

Use the **no** variant of this command to remove the AMF area.

This command is only valid on AMF controllers, master nodes and gateway nodes.

Syntax

```
atmf area <area-name> id <1-4094> [local]
no atmf area <area-name>
```

Parameter	Description
<area-name>	The AMF area name. The area name can be up to 15 characters long. Valid characters are: a..z A..Z 0..9 - _ Names are case sensitive and must be unique within an AMF network. The name cannot be the word "local" or an abbreviation of the word "local" (such as "l", "lo" etc.).
<1-4094>	An ID number that uniquely identifies this area.
`local`	Set the area to be the local area. The local area contains the device you are configuring.

Mode Global Configuration

Usage notes This command enables you to divide your AMF network into areas. Each area is managed by at least one AMF master node. Each area can have up to 120 nodes, depending on the license installed on that area's master node.

The whole AMF network is managed by up to 8 AMF controllers. Each AMF controller can communicate with multiple areas. The number of areas supported on a controller depends on the license installed on that controller.

You must give each area in an AMF network a unique name and ID number.

Only one local area can be configured on a device. You must specify a local area on each controller, remote AMF master, and gateway node.

Example To create the AMF area named New-Zealand, with an ID of 1, and specify that it is the local area, use the command:

```
controller-1(config)# atmf area New-Zealand id 1 local
```

To configure a remote area named Auckland, with an ID of 100, use the command:

```
controller-1(config)# atmf area Auckland id 100
```

Related commands

atmf area password

show atmf area

show atmf area summary

show atmf area nodes

switchport atmf-arealink

Command changes

Version 5.5.1-2.1: area **id** maximum increased to 4094

atmf area password

Overview This command sets a password on an AMF area.

Use the **no** variant of this command to remove the password.

This command is only valid on AMF controllers, master nodes and gateway nodes. The area name must have been configured first.

Syntax

```
atmf area <area-name> password [8] <password>
no atmf area <area-name> password
```

Parameter	Description
<area-name>	The AMF area name.
8	This parameter is displayed in **show running-config** output to indicate that it is displaying the password in encrypted form. You should not enter **8** on the CLI yourself.
<password>	The password is between 8 and 32 characters long. It can include spaces.

Mode Global Configuration

Usage notes You must configure a password on each area that an AMF controller communicates with, except for the controller's local area. The areas must already have been created using the atmf area command.

Enter the password identically on both of:

- the area that locally contains the controller, and
- the remote AMF area masters

The command **show running-config atmf** will display the encrypted version of this password. The encryption keys will match between the controller and the remote AMF master.

If multiple controller and masters exist in an area, they must all have the same area configuration.

Example To give the AMF area named *Auckland* a password of "secure#1" use the following command on the controller:

```
controller-1(config)# atmf area Auckland password secure#1
```

and also use the following command on the master node for the Auckland area:

```
auck-master(config)# atmf area Auckland password secure#1
```

Related commands

atmf area

show atmf area

show atmf area summary

show atmf area nodes

switchport atmf-arealink

atmf authorize

Overview On an AMF network, with secure mode enabled, use this command on an AMF master to authorize an AMF node to join the network. AMF nodes waiting to be authorized appear in the pending authorization queue, which can be examined using the show atmf authorization command with the **pending** parameter.

Use the **no** variant of this command to revoke authorization for an AMF node on an AMF master.

Syntax

```
atmf authorize {<node-name> [area <area-name>]|all-pending}
no atmf authorize <node-name> [area <area-name>]
```

Parameter	Description
<node-name>	The name of the node to be authorized or have its authorization revoked.
area	Specify an AMF area.
<area-name>	This is the name of the area the node belongs to.
all-pending	Authorize all nodes in the pending queue.

Mode Privileged Exec

Usage notes On an AMF controller, AMF remote-area masters must be authorized by the controller, and the AMF remote-area masters will also need to authorized access from the AMF controller.

Example To authorize all AMF nodes in the pending authorization queue on an AMF master, use the command:

```
awplus# atmf authorize all-pending
```

To authorize a node called “node2” in remote AMF area “area3”, use the command:

```
awplus# atmf authorize node2 area “area3”
```

To authorize a node called “node4” on an AMF master, use the command:

```
awplus# atmf authorize node4
```

To revoke authorization for a node called “node4” on an AMF master, use the command:

```
awplus# no atmf authorize node4
```

Related commands

atmf secure-mode

clear atmf secure-mode certificates

show atmf authorization

show atmf secure-mode

show atmf secure-mode certificates

show atmf secure-mode statistics

Command changes Version 5.4.7-0.3: command added

atmf authorize provision

Overview Use this command from an AMF controller or AMF master to pre-authorize a node on an AMF network running in secure mode. This allows a node to join the AMF network the moment the atmf secure-mode command is run on that node.

Use the **no** variant of this command to remove a provisional authorization from and AMF controller or AMF master.

Syntax

```
atmf authorize provision [timeout <minutes>] node <node-name>
interface <interface-name> [area <area-name>]
atmf authorize provision [timeout <minutes>] mac <mac-address>
atmf authorize provision [timeout <minutes>] all
no atmf authorize provision node <node-name> interface
<interface-name> [area <area-name>]
no atmf authorize provision mac <mac-address>
no atmf authorize provision all
```

Parameter	Description
`timeout`	Timeout for provisional authorization. Authorization for provisioned nodes expires after the timeout period specified.
<minutes>	Timeout in minutes. A value between 1 and 6000 is permissible with the default being 60 minutes.
`node`	Specify a node to provision by node name.
<node-name>	The name of the node to provisionally authorize.
`interface`	Specify the interface the node will connect on.
<interface-name>	The name of the interface, this can be a switchport, link aggregator, LACP link, or virtual link.
`area`	Specify the AMF area.
<area-name>	This is the name of the area the node belongs to.
`mac`	Specify a node to provision by MAC address.
<mac-address>	Enter a MAC address to provisionally authorize in the format HHHH.HHHH.HHHH.
`all`	Provision authorization for all secure mode capable nodes.

Default The default timeout is 60 minutes.

Mode Privileged Exec

Example To provisionally authorize all non-secure AMF nodes, use the command:

```
awplus# atmf authorize provision all
```

To authorize a node with a MAC address of 0000.cd28.0880 for 2 hours, use the command:

```
awplus# authorize provision timeout 120 mac 0000.cd28.0880
```

To remove all provisional authorization, on an AMF master, use the command:

```
awplus# no atmf authorize provision all
```

Related commands

show atmf authorization

show atmf secure-mode

Command changes

Version 5.4.7-0.3: command added

atmf backup

Overview This command can only be applied to a master node. It manually schedules an AMF backup to start at a specified time and to execute a specified number of times per day.

Use the **no** variant of this command to disable the schedule.

Syntax

```
atmf backup {default|<hh:mm> frequency <1-24>}
```

Parameter	Description
`default`	Restore the default backup schedule.
`<hh:mm>`	Sets the time of day to apply the first backup, in hours and minutes. Note that this parameter uses the 24 hour clock.
`backup`	Enables AMF backup to external media.
`frequency <1-24>`	Sets the number of times within a 24 hour period that backups will be taken.

Default Backups run daily at 03:00 AM, by default

Mode Global Configuration

Usage notes Running this command only configures the schedule. To enable the schedule, you should then apply the command atmf backup enable.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

Example To schedule backup requests to begin at 11 am and execute twice per day (11 am and 11 pm), use the following command:

```
node_1# configure terminal
node_1(config)# atmf backup 11:00 frequency 2
```

CAUTION: *File names that comprise identical text, but with differing case, such as Test.txt and test.txt, will not be recognized as being different on FAT32 based backup media such as a USB storage device. However, these filenames will be recognized as being different on your Linux based device. Therefore, for good practice, ensure that you apply a consistent case structure for your back-up file names.*

Related commands atmf backup enable

atmf backup stop

show atmf backup

atmf backup area-masters delete

Overview Use this command to delete from external media, a backup of a specified node in a specified area.

Note that this command can only be run on an AMF controller.

Syntax

```
atmf backup area-masters delete area <area-name> node
<node-name>
```

Parameter	Description
<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 AMF area named Wellington, use the command:

```
controller-1# atmf backup area-masters delete area Wellington
node well-gate
```

Related commands show atmf backup area

atmf backup area-masters enable

Overview Use this command to enable backup of remote area-masters from the AMF controller. This command is only valid on AMF controllers.

Use the **no** form of the command to stop backups of remote area-masters.

Syntax

```
atmf backup area-masters enable
no atmf backup area-masters enable
```

Mode Global configuration

Default Remote area backups are disabled by default

Usage notes Use the following commands to configure the remote area-master backups:

- atmf backup to configure when the backups begin and how often they run
- atmf backup server to configure the backup server.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

Example To enable scheduled backups of AMF remote area-masters, use the commands:

```
controller-1# configure terminal
controller-1(config)# atmf backup area-masters enable
```

To disable scheduled backups of AMF remote area-masters, use the commands:

```
controller-1# configure terminal
controller-1(config)# no atmf backup area-masters enable
```

Related commands

atmf backup server

atmf backup

show atmf backup area

atmf backup area-masters now

Overview Use this command to run an AMF backup of one or more remote area-masters from the AMF controller immediately.

This command is only valid on AMF controllers.

Syntax

```
atmf backup area-masters now [area <area-name>|area <area-name>
node <node-name>]
```

Parameter	Description
<area-name>	The area whose area-masters will be backed up.
<node-name>	The node that will be backed up.

Mode Privileged Exec

Example To back up all local master nodes in all areas controlled by controller-1, use the command

```
controller-1# atmf backup area-masters now
```

To back up all local masters in the AMF area named Wellington, use the command

```
controller-1# atmf backup area-masters now area Wellington
```

To back up the local master “well-master” in the Wellington area, use the command

```
controller-1# atmf backup area-masters now area Wellington node
well-master
```

Related commands

atmf backup area-masters enable

atmf backup area-masters synchronize

show atmf backup area

atmf backup area-masters synchronize

Overview Use this command to synchronize backed-up area-master files between the active remote file server and the backup remote file server. Files are copied from the active server to the remote server.

Note that this command is only valid on AMF controllers.

Syntax
```
atmf backup area-masters synchronize
```

Mode Privileged Exec

Example To synchronize backed-up files between the remote file servers for all area-masters, use the command:

```
controller-1# atmf backup area-masters synchronize
```

Related commands
- atmf backup area-masters enable
- atmf backup area-masters now
- show atmf backup area

atmf backup bandwidth

Overview This command sets the maximum bandwidth in kilobytes per second (kBps) available to the AMF backup process. This command enables you to restrict the bandwidth that is utilized for downloading file contents during a backup.

NOTE: *This command will only run on an AMF master. An error message will be generated if the command is attempted on node that is not a master.*

Also note that setting the bandwidth value to zero will allow the transmission of as much bandwidth as is available, which can exceed the maximum configurable speed of 1000 kBps. In effect, zero means unlimited.

Use the **no** variant of this command to reset (to its default value of zero) the maximum bandwidth in kilobytes per second (kBps) available when initiating an AMF backup. A value of zero tells the backup process to transfer files using unlimited bandwidth.

Syntax

```
atmf backup bandwidth <0-1000>
no atmf backup bandwidth
```

Parameter	Description
<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.

Note that this command can only be run from an AMF master node.

Syntax

```
atmf backup delete <node-name>
```

Parameter	Description
<node-name>	The AMF node name of the backup file to be deleted.

Mode Privileged Exec

Example To delete the backup file from node2, use the following command:

```
Node_1# atmf backup delete node2
```

Related commands

show atmf backup

atmf backup now

atmf backup stop

atmf backup enable

Overview This command enables automatic AMF backups on the AMF master node that you are connected to. By default, automatic backup starts at 3:00 AM. However, this schedule can be changed by the atmf backup command. Note that backups are initiated and stored only on the master nodes.

Use the **no** variant of this command to disable any AMF backups that have been scheduled and previously enabled.

Syntax

```
atmf backup enable
no atmf backup enable
```

Default Automatic AMF backup functionality is enabled on the AMF master when it is configured and external media, i.e. an SD card or a USB storage device or remote server, is detected.

Mode Global Configuration

Usage notes A warning message will appear if you run the atmf backup enable command with either insufficient or marginal memory availability on your external storage device.

You can use the command show atmf backup on page 739 to check the amount of space available on your external storage device.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

Example To turn on automatic AMF backup, use the following command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup enable
```

Related commands

show atmf

show atmf backup

atmf backup

atmf backup now

atmf enable

atmf backup guests delete

Overview This command removes a guest node's backup files from external media such as a USB drive, SD card, or an external file server.

Syntax

```
atmf backup guests delete <node-name> <guest-port>
```

Parameter	Description
<node-name>	The name of the guest's parent node.
<guest-port>	The port number on the parent node.

Mode User Exec/Privileged Exec

Example On a parent node named "node1" (which, in this case, the user has a direct console connection to) use the following command to remove the backup files of the guest node that is directly connected to port1.0.3.

```
node1# atmf backup guests delete node1 port1.0.3
```

Related Command

atmf backup delete

atmf backup area-masters delete

show atmf backup guest

atmf backup guests enable

Overview Use this command to enable backups of remote guest nodes from an AMF master.

Use the **no** variant of this command to disable the ability of the guest nodes to be backed up.

Syntax

```
atmf backup guests enable
no atmf backup guests enable
```

Default Guest node backups are enabled by default.

Mode Global Config

Usage notes We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

Example On the AMF master node, enable all scheduled guest node backups:

```
atmf-master# configure terminal
atmf-master(config)# atmf backup guests enable
```

Related commands

atmf backup area-masters enable

show atmf backup guest

atmf backup guests synchronize

atmf backup guests now

Overview This command manually triggers an AMF backup of guest nodes on a AMF Master.

Syntax

```
atmf backup guests now [<node-name>] [<guest-port>]
```

Parameter	Description
<node-name>	The name of the guest's parent node.
<guest-port>	The port number that connects to the guest node.

Default n/a

Mode Privileged Exec

Example Use the following command to manually trigger the backup of all guests in the AMF network

```
awplus# atmf backup guests now
```

Example To manually trigger the backup of a guest node connected to port 1.0.23 of node1, use the following command:

```
awplus# atmf backup guests now node1 port1.0.23
```

Related commands show atmf backup guest

atmf backup guests synchronize

Overview This command initiates a manual synchronization of all guest backup file-sets across remote file servers and various redundancy backup media, such as USB storage devices. This facility ensures that each device contains the same backup image files. Note that this backup synchronization process will occur as part of the regular backups scheduled by the atmf backup command.

Syntax
```
atmf backup guests synchronize
```

Default n/a

Mode User Exec/Privileged Exec

Example To synchronize backups across remote file servers and storage devices, use the command:

```
Node1#atmf backup guests synchronize
```

Related commands atmf backup redundancy enable

show atmf guests

atmf backup guests enable

atmf backup now

Overview This command initiates an immediate AMF backup of either all AMF members, or a selected AMF member. Note that this backup information is stored in the external media on the master node of the device on which this command is run, even though the selected AMF member may not be a master node.

Note that this command can only be run on an AMF master node.

Syntax

```
atmf backup now [<nodename>]
```

Parameter	Description
<nodename> or *<hostname>*	The name of the AMF member to be backed up, as set by the command hostname on page 171. 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 notes Although this command will select the AMF node to be backed-up, it can only be run from any AMF master node.

NOTE: *The backup produced will be for the selected node but the backed-up config will reside on the external media of the AMF master node on which the command was run. However, this process will result in the information on one master being more up-to-date. To maintain concurrent backups on both masters, you can apply the backup now command to the master working-set. This is shown in Example 4 below.*

Example 1 In this example, an AMF member has not been assigned a host name. The following command is run on the AMF_Master_2 node to immediately backup the device that is identified by its MAC address of 0016.76b1.7a5e:

```
AMF_Master_2# atmf backup now host_0016_76b1_7a5e
```

NOTE: *When a host name is derived from its MAC address, the syntax format entered changes from XXXX.XXXX.XXXX to XXXX_XXXX_XXXX.*

Example 2 In this example, an AMF member has the host name, **office_annex**. The following command will immediately backup this device:

```
AMF_Master_2# atmf backup now office_annex
```

This command is initiated on the device's master node named **AMF_Master_2** and initiates an immediate backup on the device named **office_annex**.

Example 3 To initiate from AMF_master_1 an immediate backup of all AMF member nodes, use the following command:

```
AMF_Master_1# amf backup now
```

Example 4 To initiate an immediate backup of the node with the host-name “office_annex” and store the configuration on both masters, use the following process:

From the AMF_master_1, set the working-set to comprise only of the automatic group, master nodes.

```
AMF_Master_1# atmf working-set group master
```

This command returns the following display:

```
============================
AMF_Master_1, AMF_Master_2
============================

Working set join
```

Backup the AMF member with the host name, **office_annex** on both the master nodes as defined by the working set.

```
AMF_Master[2]# atmf backup now office_annex
```

Note that the [2] shown in the command prompt indicates a 2 node working-set.

Related commands

atmf backup

atmf backup stop

hostname

show atmf backup

atmf backup redundancy enable

Overview This command is used to enable or disable AMF backup redundancy.

Syntax

```
atmf backup redundancy enable
no atmf backup redundancy enable
```

Default Disabled

Mode Global Configuration

Usage notes If the AMF Master or Controller supports any removable media (SD card/USB), it uses the removable media as the redundant backup for the AMF data backup.

This feature is valid only if remote file servers are configured on the AMF Master or Controller.

We recommend using the ext3 or ext4 filesystem on external media that are used for AMF backups.

Example To enable AMF backup redundancy, use the commands:

```
awplus# configure terminal
awplus(config)# atmf backup redundancy enable
```

To disable AMF backup redundancy, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf backup redundancy enable
```

Related commands

atmf backup synchronize

show atmf backup

show atmf backup area

atmf backup server

Overview This command configures remote file servers as the destination for AMF backups.

Use the **no** variant of this command to remove the destination server(s). When all servers are removed the system will revert to backup from external media.

Syntax

```
atmf backup server id {1|2} <hostlocation> username <username>
[path <path>|port <1-65535>]
```

```
no atmf backup server id {1|2}
```

Defaults Remote backup servers are not configured. The default SSH TCP port is 22. The path utilized on the remote file server is the home directory of the username.

Mode Global Exec

Usage notes The hostname and username parameters must both be configured.

Examples To configure server 1 with an IPv4 address and a username of *backup1*, use the commands:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 192.168.1.1
username backup1
```

To configure server 1 with an IPv6 address and a username of *backup1*, use the command:

```
AMF_backup1_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 FFEE::01 username
backup1
```

To configure server 2 with a hostname and username, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com
username backup2
```

To configure server 2 with a hostname and username in addition to the optional path and port parameters, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com
username backup2 path tokyo port 1024
```

To unconfigure the AMF remote backup file server 1, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# no atmf backup server id 1
```

Related commands show atmf backup

atmf backup stop

Overview Running this command stops a backup that is currently running on the master node you are logged onto. Note that if you have two masters and want to stop both, then you can either run this command separately on each master node, or add both masters to a working set, and issue this command to the working set.

Note that this command can only be run on a master node.

Syntax

```
atmf backup stop
```

Mode Privileged Exec

Usage notes This command is used to halt an AMF backup that is in progress. In this situation the backup process will finish on its current node and then stop.

Example To stop a backup that is currently executing on master node node-1, use the following command:

```
AMF_Master_1# amf backup stop
```

Related commands

atmf backup

atmf backup enable

atmf backup now

show atmf backup

atmf backup synchronize

Overview For the master node you are connected to, this command initiates a system backup of files from the node's active remote file server to its backup remote file server. Note that this process happens automatically each time the network is backed up.

Note that this command can only be run from a master node.

Syntax

```
atmf backup synchronize
```

Mode Privileged Exec

Example When connected to the master node AMF_Master_1, the following command will initiate a backup of all system related files from its active remote file server to its backup remote file server.

```
AMF_Master_1# atmf backup synchronize
```

Related commands

atmf backup enable

atmf backup redundancy enable

show atmf

show atmf backup

atmf cleanup

Overview This command is an alias to the erase factory-default command.

atmf container

Overview Use this command to create or update an AMF container on a Virtual AMF Appliance (VAA) virtual machine.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the AMF Feature Overview and Configuration Guide for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove an AMF container.

Syntax

```
atmf container <container-name>
no atmf container <container-name>
```

Parameter	Description
<container-name>	The name of the AMF container to create, update, or remove.

Mode AMF Container Configuration

Usage notes You cannot delete a container while it is still running. First use the **state disable** command to stop the container.

Examples To create or update the AMF container “vac-wlg-1”, use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)#
```

To remove the AMF container “vac-wlg-1”, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf container vac-wlg-1
```

Related commands

area-link

atmf container login

bridge-group (amf-container)

description (amf-container)

show atmf container

state

Command changes Version 5.4.7-0.1: command added

atmf container login

Overview Use this command to login to an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the AMF Feature Overview and Configuration Guide for more information on running multiple tenants on a single VAA host.

Syntax

```
atmf container login <container-name>
```

Parameter	Description
<container-name>	The name of the AMF container you wish to login into.

Mode Privileged Exec

Usage notes If you try to login to a AMF container that has not been created, or is not running, you will see the following message:

```
% Container does not exist or is not running.
```

To exit from a container and return to the host VAA press <Ctrl+a q>.

Example To login to container "vac-wlg-1", use the command:

```
awplus# atmf container login vac-wlg-1
```

You will then be presented with a login screen for that container:

```
Connected to tty 1
Type <Ctrl+a q> to exit the console, <Ctrl+a Ctrl+a> to enter Ctrl+a itself

vac-wlg-1 login: manager
Password: friend

AlliedWare Plus (TM) 5.4.7 02/03/17 08:46:12

vac-wlg-1>
```

Related commands atmf container

show atmf container

Command changes Version 5.4.7-0.1: command added

atmf controller

Overview Use this command to configure the device as an AMF controller. This enables you to split a large AMF network into multiple areas.

AMF controller is a licensed feature. The number of areas supported on a controller depends on the license installed on that controller.

Use the **no** variant of this command to remove the AMF controller functionality.

Syntax

```
atmf controller
no atmf controller
```

Mode Global configuration

Usage notes If a valid AMF controller license is not available on the device, the device will accept this command but will not act as a controller until you install a valid license. The following message will warn you of this:

"An AMF Controller license must be installed before this feature will become active"

NOTE: *If the AMF controller functionality is removed from a device using the* ***no atmf controller*** *command then the device must be rebooted if it is to function properly as an AMF master.*

Example To configure the node named *controller-1* as an AMF controller, use the commands:

```
controller-1# configure terminal
controller-1(config)# atmf controller
```

To stop the node named *controller-1* from being an AMF controller, use the commands:

```
controller-1# configure terminal
controller-1(config)# no atmf controller
```

Related commands atmf area

show atmf

atmf distribute firmware

Overview This command can be used to upgrade software one AMF node at a time. A URL can be selected from any media location. The latest compatible release for a node will be selected from this location.

Several procedures are performed to ensure the upgrade will succeed. This includes checking the current node release boots from flash. If there is enough space on flash, the software release is copied to flash on the new location.

The new release name is updated using the **boot system** command. The old release will become the backup release file. If a release file exists in a remote device (such as TFTP or HTTP, for example) then the URL should specify the exact release filename without using a wild card character.

The command will continue to upgrade software until all nodes are upgraded. At the end of the upgrade cycle the command should be used on the working-set.

Syntax `atmf distribute firmware <filename>`

Parameter	Description
<filename>	The filename and path of the file. See the File Management Feature Overview and Configuration Guide for valid syntax.

Mode Privileged Exec

Examples To upgrade nodes in a AMF network with a predefined AMF group called 'teams', use the following command:

```
Team1# atmf working-set group teams
```

```
============================
Team1, Team2, Team3:
============================
Working set join
```

```
ATMF_NETWORK[3]# atmf distribute firmware card:*.rel
```

```
Retrieving data from Team1
Retrieving data from Team2
Retrieving data from Team3

ATMF Firmware Upgrade:

Node Name          New Release File           Status
-----------------------------------------------------------------
Team1              x510-5.4.7-1.1.rel         Release ready
Team2              x930-5.4.7-1.1.rel         Release ready
Team3              x930-5.4.7-1.1.rel         Release ready
Continue the rolling reboot ? (y/n):y
=================================================================
Copying Release    : x510-5.4.7-1.1.rel to Team1
Updating Release   : x510-5.4.7-1.1.rel information on Team1
=================================================================
Copying Release    : x930-5.4.7-1.1.rel to Team2
Updating Release   : x930-5.4.7-1.1.rel information on Team2
=================================================================
Copying Release    : x930-5.4.7-1.1.rel to Team3
Updating Release   : x930-5.4.7-1.1.rel information on Team3

=================================================================
New firmware will not take effect until nodes are rebooted.
=================================================================

ATMF_NETWORK[3]#
```

Related commands atmf working-set

atmf domain vlan

Overview The AMF domain VLAN is created when the AMF network is first initiated and is assigned a default VID of 4091. This command enables you to change the VID from this default value on this device.

The AMF domain VLAN is one of AMF's internal VLANs (the management VLAN is the other internal VLAN). AMF uses these internal VLANs to communicate network status information between nodes. These VLANs must be reserved for AMF and not used for other purposes.

An important point conceptually is that although the domain VLAN exists globally across the AMF network, it is assigned separately to each domain. The AMF network therefore can be thought of as comprising a series of domain VLANs each having the same VID and each being applied to a horizontal slice (domain) of the AMF. It follows therefore that the domain VLANs are only applied to ports that form cross-links and not to ports that form uplinks/downlinks.

CAUTION: *Every member of your AMF network must have the same domain VLAN, management VLAN, and management subnet.*

CAUTION: *If you change the domain VLAN, management VLAN, or management subnet of a node, that change takes effect immediately and the node will immediately leave the AMF network and try to rejoin it. The AMF network will not be complete until you have given all devices the same setting, so they can all rejoin the AMF network.*

Use the **no** variant of this command to reset the VLAN ID to its default value of 4091.

Syntax

```
atmf domain vlan <2-4090>
no atmf domain vlan
```

Parameter	Description
<2-4090>	The VLAN number in the range 2 to 4090.

Default VLAN 4091

Mode Global Configuration

Usage notes We recommend you only change the domain VLAN when first creating the AMF network, and only if VLAN 4091 is already being used in your network.

However, if you do need to change the VLAN on an existing AMF network, use the following steps:

1) Create a working set of the whole of your AMF network, using the commands:

```
master# atmf working-set group all
```

You must use **working-set group all** if changing the domain VLAN. If you use a different working-set, nodes that are not in that working-set will lose contact with the AMF network.

2) The prompt will display the number of nodes in the AMF network. Record this number. In this example, the network is named “test” and has 10 nodes:

```
test[10]#
```

3) Enter the new VLAN ID, using the commands:

```
test[10]# configure terminal
test(config)[10]# atmf domain vlan <2-4090>
```

The nodes will execute the command in parallel, leave the AMF network, and attempt to rejoin through the new VLAN.

4) Create the working set again, using the commands:

```
master(config)# exit
master# atmf working-set group all
```

5) Save the configuration, using the command:

```
test[10]# write
```

6) The prompt will display the number of nodes in the AMF network. Check that this is the same as the number in step 1. If it is not, you will need to change the VLAN on missing devices by logging into their consoles directly.

NOTE: *The domain VLAN will automatically be assigned an IP subnet address based on the value configured by the command atmf management subnet.*

The default VLAN ID lies outside the user-configurable range. If you need to reset the VLAN to the default VLAN ID, use the **no** variant of this command to do so.

Examples To change the AMF domain VLAN to 4090 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# atmf domain vlan 4090
master(config)# exit
master# atmf working-set group all
test[10]# write
```

To reset the AMF domain VLAN to its default of 4091in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# no atmf domain vlan
master(config)# exit
master# atmf working-set group all
test[10]# write
```

Related commands

atmf management subnet

atmf management vlan

atmf enable

Overview This command manually enables (turns on) the AMF feature for the device being configured.

Use the **no** variant of this command to disable (turn off) the AMF feature on the member node.

Syntax

```
atmf enable
no atmf enable
```

Default Once AMF is configured, the AMF feature starts automatically when the device starts up.

Mode Global Configuration

Usage notes The device does not auto negotiate AMF domain specific settings such as the Network Name. You should therefore, configure your device with any domain specific (non default) settings before enabling AMF.

Examples To turn off AMF, use the command:

```
MyNode# config terminal
MyNode(config)# no atmf enable
```

To turn on AMF, use the command:

```
MyNode(config)# atmf enable
```

This command returns the following display:

```
% Warning: The ATMF network config has been set to enable
% Save the config and restart the system for this change to take
effect.
```

atmf group (membership)

Overview This command configures a device to be a member of one or more AMF groups. Groups exist in three forms: Implicit Groups, Automatic Groups, and User-defined Groups.

- Implicit Groups
  - all: All nodes in the AMF
  - current: The current working-set
  - local: The originating node.

Note that the Implicit Groups do not appear in show group output.

- Automatic Groups - These are defined by hardware architecture, e.g. x510, x230, x8100, AR3050S, AR4050S.
- User-defined Groups - These enable you to define arbitrary groups of AMF members based on your own criteria.

Each node in the AMF is automatically assigned membership to the implicit groups, and the automatic groups that are appropriate to its node type, e.g. x230, PoE. Similarly, nodes that are configured as masters are automatically assigned to the master group.

Use the **no** variant of this command to remove the membership.

Syntax

```
atmf group <group-list>
no atmf group <group-list>
```

Parameter	Description
<group-list>	A list of group names. These should be entered as a comma delimited list without spaces. Names can contain alphanumeric characters, hyphens and underscores.

Mode Global Configuration

Usage notes You can use this command to define your own arbitrary groups of AMF members based on your own network's configuration requirements. Applying a node to a non existing group will result in the group automatically being created.

Note that the master nodes are automatically assigned to be members of the pre-existing master group.

The following example configures the device to be members of three groups; two are company departments, and one comprises all devices located in building_2. To avoid having to run this command separately on each device that is to be added to these groups, you can remotely assign all of these devices to a working-set, then use the capabilities of the working-set to apply the atmf group (membership) command to all members of the working set.

Example 1 To specify the device to become a member of AMF groups named *marketing*, *sales*, and *building_2*, use the following commands:

```
node-1# configure terminal
node-1(config)# atmf group marketing,sales,building_2
```

Example 2 To add the nodes *member_node_1* and *member_node_2* to groups *building1* and *sales*, first add the nodes to the working-set:

```
master_node# atmf working-set member_node_1,member_node_2
```

This command returns the following output confirming that the nodes *member_node_1* and *member_node_2* are now part of the working-set:

```
============================
member_node_1, member_node_2
============================

Working set join
```

Then add the members of the working set to the groups:

```
atmf-net[2]# configure terminal
atmf-net[2](config)# atmf group building1,sales
atmf-net[2](config)# exit
atmf-net[2]# show atmf group
```

This command returns the following output displaying the groups that are members of the working-set.

```
====================
member_node_1
====================

AMF group information

building1, sales
```

Related commands

show atmf group

show atmf group members

atmf guest-class

Overview This modal command creates a guest-class. Guest-classes are modal templates that can be applied to selected guest types. Once you have created a guest-class, you can select it by entering its mode. From here, you can then configure a further set of operational settings specifically for the new guest-class.

These settings can then all be applied to a guest link by running the switchport atmf-guestlink command. The following settings can be configured from each guest class mode:

- discovery method
- model type
- http-enable setting
- guest port, user name, and password

The **no** variant of this command removes the guest-class. Note that you cannot remove a guest-class that is assigned to a port.

Syntax

```
atmf guest-class <guest-class-name>
no atmf guest-class <guest-class-name>
```

Parameter	Description
<guest-class-name>	The name assigned to the guest-class type. This can be chosen from an arbitrary string of up to 15 characters.

Mode Global Configuration

Example To create a guest-class named 'camera' use the commands:

```
node1# configure terminal
node1(config)# atmf guest-class camera
node1(config-atmf-guest)#
```

To remove the guest-class named 'camera' use the commands:

```
node1# configure terminal
node1(config)# no atmf guest-class camera
```

Related commands

show atmf area guests

discovery

firmware-url

http-enable

username (atmf-guest)

modeltype

switchport atmf-guestlink

show atmf links guest

show atmf guests

login-fallback enable

atmf log-verbose

Overview Use the **no** variant of this command to reset to the default.

atmf management subnet

Overview This command is used to assign a subnet that will be allocated to the AMF management and domain management VLANs. From the address space defined by this command, two subnets are created, a management subnet component and a domain component, as explained in the Usage section below.

AMF uses these internal IPv4 subnets to communicate network status information between nodes. These subnet addresses must be reserved for AMF and not used for other purposes.

CAUTION: *Every member of your AMF network must have the same domain VLAN, management VLAN, and management subnet.*

CAUTION: *If you change the domain VLAN, management VLAN, or management subnet of a node, that change takes effect immediately and the node will immediately leave the AMF network and try to rejoin it. The AMF network will not be complete until you have given all devices the same setting, so they can all rejoin the AMF network.*

Use the **no** variant of this command to remove the assigned subnet.

Syntax

```
atmf management subnet <a.b.0.0>
no atmf management subnet
```

Parameter	Description
<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 notes Running this command will result in the creation of a further two subnets (within the class B address space assigned) and the mask will extend from /16 to /17.

For example, if the management subnet is assigned the address 172.31.0.0/16, this will result in the automatic creation of the following two subnets:

- 172.31.0.0/17 assigned to the atmf management vlan
- 172.31.128.0/17 assigned to the atmf domain vlan.

We recommend you only change the management subnet when first creating the AMF network, and only if 172.31.0.0 is already being used in your network.

However, if you do need to change the subnet on an existing AMF network, use the following steps:

1) Create a working set of the whole of your AMF network, using the commands:

```
master# atmf working-set group all
```

You must use **working-set group all** if changing the domain VLAN, management VLAN, or management subnet. If you use a different working-set, nodes that are not in that working-set will lose contact with the AMF network.

2) The prompt will display the number of nodes in the AMF network. Record this number. In this example, the network is named “test” and has 10 nodes:

```
test[10]#
```

3) Enter the new subnet address, using the commands:

```
test[10]# configure terminal
test(config)[10]# atmf management subnet <a.b.0.0>
```

The nodes will execute the command in parallel, leave the AMF network, and attempt to rejoin through the new subnet.

4) Create the working set again, using the commands:

```
master(config)# exit
master# atmf working-set group all
```

5) Save the configuration, using the command:

```
test[10]# write
```

6) The prompt will display the number of nodes in the AMF network. Check that this is the same as the number in step 1. If it is not, you will need to change the subnet on missing devices by logging into their consoles directly.

Examples To change the AMF management subnet address to 172.25.0.0 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# atmf management subnet 172.25.0.0
master(config)# exit
master# atmf working-set group all
test[10]# write
```

To reset the AMF management subnet address to its default of 172.31.0.0 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# no atmf management subnet
master(config)# exit
master# atmf working-set group all
test[10]# write
```

Related commands

atmf domain vlan

atmf management vlan

atmf management vlan

Overview The AMF management VLAN is created when the AMF network is first initiated and is assigned a default VID of 4092. This command enables you to change the VID from this default value on this device.

The AMF management VLAN is one of AMF's internal VLANs (the domain VLAN is the other internal VLAN). AMF uses these internal VLANs to communicate network status information between nodes. These VLANs must be reserved for AMF and not used for other purposes.

CAUTION: *Every member of your AMF network must have the same domain VLAN, management VLAN, and management subnet.*

CAUTION: *If you change the domain VLAN, management VLAN, or management subnet of a node, that change takes effect immediately and the node will immediately leave the AMF network and try to rejoin it. The AMF network will not be complete until you have given all devices the same setting, so they can all rejoin the AMF network.*

Use the **no** variant of this command to restore the VID to the default of 4092.

Syntax

```
atmf management vlan <2-4090>
no atmf management vlan
```

Parameter	Description
<2-4090>	The VID assigned to the AMF management VLAN.

Default VLAN 4092

Mode Global Configuration

Usage notes We recommend you only change the management VLAN when first creating the AMF network, and only if VLAN 4092 is already being used in your network.

However, if you do need to change the VLAN on an existing AMF network, use the following steps to ensure you change it on all nodes simultaneously:

1) Create a working set of the whole of your AMF network, using the commands:

```
master# atmf working-set group all
```

You must use **working-set group all** if changing the management VLAN. If you use a different working-set, nodes that are not in that working-set will lose contact with the AMF network.

2) The prompt will display the number of nodes in the AMF network. Record this number. In this example, the network is named "test" and has 10 nodes:

```
test[10]#
```

3) Enter the new VLAN ID, using the commands:

```
test[10]# configure terminal
test(config)[10]# atmf management vlan <2-4090>
```

The nodes will execute the command in parallel, leave the AMF network, and attempt to rejoin through the new VLAN.

4) Create the working set again, using the commands:

```
master(config)# exit
master# atmf working-set group all
```

5) Save the configuration, using the command:

```
test[10]# write
```

6) The prompt will display the number of nodes in the AMF network. Check that this is the same as the number in step 1. If it is not, you will need to change the VLAN on missing devices by logging into their consoles directly.

NOTE: *The management VLAN will automatically be assigned an IP subnet address based on the value configured by the command atmf management subnet.*

The default VLAN ID lies outside the user-configurable range. If you need to reset the VLAN to the default VLAN ID, use the **no** variant of this command to do so.

Examples To change the AMF management VLAN to 4090 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# atmf management vlan 4090
master(config)# exit
master# atmf working-set group all
test[10]# write
```

To reset the AMF management VLAN to its default of 4092 in an existing AMF network, use the following commands:

```
master# atmf working-set group all
test[10]# configure terminal
test(config)[10]# no atmf management vlan
master(config)# exit
master# atmf working-set group all
test[10]# write
```

Related commands atmf domain vlan

atmf management subnet

atmf master

Overview This command configures the device to be an AMF master node and automatically creates an AMF master group. The master node is considered to be the core of the AMF network, and must be present for the AMF to form. The AMF master has its node depth set to 0. Note that the node depth vertical distance is determined by the number of uplinks/downlinks that exist between the node and its master.

An AMF master node must be present for an AMF network to form. Up to two AMF master nodes may exist in a network, and they **must** be connected by an AMF crosslink.

NOTE: *Master nodes are an essential component of an AMF network. In order to run AMF, an AMF License is required for each master node.*

If the crosslink between two AMF masters fails, then one of the masters will become isolated from the rest of the AMF network.

Use the **no** variant of this command to remove the device as an AMF master node. The node will retain its node depth of 0 until the network is rebooted.

NOTE: *Node depth is the vertical distance (or level) from the master node (whose depth value is 0).*

Syntax

```
atmf master
no atmf master
```

Default The device is not configured to be an AMF master node.

Mode Global Configuration

Example To specify that this node is an AMF master, use the following command:

```
node-1# configure terminal
node-1(config)# atmf master
```

Related commands show atmf

show atmf group

atmf mtu

Overview This command configures the AMF network Maximum Transmission Unit (MTU). The MTU value will be applied to the AMF Management VLAN, the AMF Domain VLAN and AMF Area links.

Use the **no** variant of this command to restore the default MTU.

Syntax

```
atmf mtu <1300-1442>
no atmf mtu
```

Parameter	Description
<1300-1442>	The value of the maximum transmission unit for the AMF network, which sets the maximum size of all AMF packets generated from the device.

Default 1300

Mode Global Configuration

Usage notes The default value of 1300 will work for all AMF networks (including those that involve virtual links over IPsec tunnels). If there are virtual links over IPsec tunnels anywhere in the AMF network, we recommend not changing this default. If there are no virtual links over IPsec tunnels, then this AMF MTU value may be increased for network efficiency.

Example To change the ATMF network MTU to 1442, use the command:

```
awplus(config)# atmf mtu 1442
```

Related commands show atmf detail

atmf network-name

Overview This command applies an AMF network name to a (prospective) AMF node. In order for an AMF network to be valid, its network-name must be configured on at least two nodes, one of which must be configured as a master and have an AMF License applied. These nodes may be connected using either AMF downlinks or crosslinks.

For more information on configuring an AMF master node, see the command atmf master.

Use the **no** variant of this command to remove the AMF network name.

Syntax

```
atmf network-name <name>
no atmf network-name
```

Parameter	Description
<name>	The AMF network name. Up to 15 printable characters can be entered for the network-name.

Mode Global Configuration

Usage notes This is one of the essential commands when configuring AMF and must be entered on each node that is to be part of the AMF.

A switching node (master or member) may be a member of only one AMF network.

CAUTION: *Ensure that you enter the correct network name. Entering an incorrect name will cause the AMF network to fragment (at the next reboot).*

Example To set the AMF network name to amf_net use the command:

```
Node_1(config)# atmf network-name amf_net
```

atmf provision (interface)

Overview This command configures a specified port on an AMF node to accept a provisioned node, via an AMF link, some time in the future.

Use the **no** variant of this command to remove the provisioning on the node.

Syntax

```
atmf provision <nodename>
no atmf provision
```

Parameter	Description
<nodename>	The name of the provisioned node that will appear on the AMF network in the future.

Mode Interface Configuration for a switchport, a static aggregator, dynamic channel group or an Eth port on an AR-Series device.

Usage notes The port should be configured as an AMF link or cross link and should be 'down' to add or remove a provisioned node.

Example To provision an AMF node named node1 for port1.0.1, use the commands:

```
host1(config)# interface port1.0.1
host1(config-if)# atmf provision node1
```

Related commands

atmf provision node

clone (amf-provision)

configure boot config (amf-provision)

configure boot system (amf-provision)

copy (amf-provision)

create (amf-provision)

delete (amf-provision)

identity (amf-provision)

license-cert (amf-provision)

locate (amf-provision)

show atmf provision nodes

show atmf links

switchport atmf-link

switchport atmf-crosslink

atmf provision node

Overview Use this command to provision a replacement node for a specified interface. Node provisioning is effectively the process of creating a backup file-set on a master node that can be loaded onto a provisioned node some time in the future. This file-set is created just as if the provisioned node really existed and was connected to the network. Typically these comprise configuration, operating system, and license files etc.

You can optionally provision a node with multiple device-type backups. When a device is then attached to the network, AMF uses its device-type to find the correct configuration to use. For example you can create an x510 and an x530 provisioning configuration for a node called 'node1' and if either an x510 or an x530 is attached to that node the appropriate configuration will be used.

Use the **no** variant of this command to remove a provisioned node.

Syntax

```
atmf provision node <nodename> [device <device-type>]
no atmf provision node <nodename> [device <device-type>]
```

Parameter	Description
<nodename>	The name of the provisioned node that will appear on the AMF network.
device	Optionally specify a device type.
<device-type>	Any valid device type e.g. AR3050s, ie200, x950. For a full list of valid device types use the command **atmf provision node <nodename> device ?**.

Mode Privileged Exec

Usage notes This command creates the directory structure for the provisioned node's file-set. It also switches to the AMF provision node prompt so that the nodes backup file-set can be created or updated. This is typically done with the create (amf-provision) or clone (amf-provision) commands.

For more information on AMF provisioning, see the AMF Feature Overview and Configuration Guide..

Example To configure node named 'node1', use the command:

```
awplus# atmf provision node node1
awplus(atmf-provision)#
```

To configure a node named 'node1' for device type 'x530', use the command:

```
awplus# atmf provision node node1 device x530
awplus(atmf-provision)#
```

Related commands

atmf provision (interface)

clone (amf-provision)

configure boot config (amf-provision)

configure boot system (amf-provision)

copy (amf-provision)

create (amf-provision)

delete (amf-provision)

identity (amf-provision)

license-cert (amf-provision)

locate (amf-provision)

show atmf provision nodes

Command changes

Version 5.4.9-0.1: command added

atmf reboot-rolling

Overview This command enables you to reboot the nodes in an AMF working-set, one at a time, as a rolling sequence in order to minimize downtime. Once a rebooted node has finished running its configuration and its ports are up, it re-joins the AMF network and the next node is rebooted.

By adding the url parameter, you can also upgrade your devices' software one AMF node at a time.

The **force** parameter forces the rolling reboot to continue even if a previous node does not rejoin the AMF network. Without the **force** parameter, the unsuitable node will time-out and the rolling reboot process will stop. However, with the **force** parameter applied, the process will ignore the timeout and move on to reboot the next node in the sequence.

This command can take a significant amount of time to complete.

Syntax

```
atmf reboot-rolling [force] [<url>]
```

Parameter	Description
`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 notes You can load the software from a variety of locations. The latest compatible release for a node will be selected from your selected location, based on the parameters and URL you have entered.

For example usb:/5.5.2-2/x*-5.5.2-2-*.rel will select from the folder usb:/5.5.2-2 the latest file that matches the selection x(wildcard)-5.5.2-2-(wildcard).rel. Because x* is applied, each device type will be detected and its appropriate release file will be installed.

Other allowable entries are:

Entry	Used when loading software
card:*.rel:	from an SD card
tftp:<*ip-address*>:	from a TFTP server
usb:	from a USB flash drive
flash:	from flash memory, e.g. from one x930 switch to another
scp:	using secure copy
http:	from an HTTP file server

Several checks are performed to ensure the upgrade will succeed. These include checking the current node release boots from flash. If there is enough space on flash, the software release is copied to flash to a new location on each node as it is processed. The new release name will be updated using the **boot system**<*release-name*> command, and the old release will become the backup release file.

NOTE: *If you are using TFTP or HTTP, for example, to access a file on a remote device then the URL should specify the exact release filename without using wild card characters.*

On bootup the software release is verified. Should an upgrade fail, the upgrading unit will revert back to its previous software version. At the completion of this command, a report is run showing the release upgrade status of each node.

NOTE: *Take care when removing external media or rebooting your devices. Removing an external media while files are being written entails a significant risk of causing a file corruption.*

Example 1 To reboot all x530 nodes in an AMF network, use the commands:

```
Bld2_Floor_1# atmf working-set group x530
```

This command returns the following type of screen output:

```
====================
node1, node2, node3:
====================

Working set join

AMF_NETWORK[3]#
```

```
ATMF_NETWORK[3]# atmf reboot-rolling
```

When the reboot has completed, a number of status screens appear. The selection of these screens will depend on the parameters set.

```
Bld2_Floor_1#atmf working-set group x530

============================
SW_Team1, SW_Team2, SW_Team3:
============================

Working set join

ATMF_NETWORK[3]#atmf reboot-rolling
ATMF Rolling Reboot Nodes:

                    Timeout
Node Name           (Minutes)
--------------------------
SW_Team1               14
SW_Team2                8
SW_Team3                8
Continue the rolling reboot ? (y/n):y
================================================
ATMF Rolling Reboot: Rebooting SW_Team1
================================================

% SW_Team1 has left the working-set
Reboot of SW_Team1 has completed
================================================
ATMF Rolling Reboot: Rebooting SW_Team2
================================================

% SW_Team2 has left the working-set
Reboot of SW_Team2 has completed
================================================
ATMF Rolling Reboot: Rebooting SW_Team3
================================================

% SW_Team3 has left the working-set
Reboot of SW_Team3 has completed

================================================
ATMF Rolling Reboot Complete
Node Name           Reboot Status
---------------------------------
SW_Team1              Rebooted
SW_Team2              Rebooted
SW_Team3              Rebooted
================================================
```

Example 2 To update firmware on all relevant devices in the network, when the new files are for 5.5.2-2.1 and are stored in a directory on a USB stick, use the commands:

```
Node_1# atmf working-set group all

ATMF_NETWORK[9]# atmf reboot-rolling
usb:/5.5.2-2/x*-5.5.2-2*.rel
```

```
ATMF Rolling Reboot Nodes:

                    Timeout
Node Name           (Minutes)    New Release File             Status
-------------------------------------------------------------------------
SW_Team1               8         x530-5.5.2-2.1.rel           Release Ready
SW_Team2              10         x530-5.5.2-2.1.rel           Release Ready
SW_Team3               8         ---                          Not Supported
HW_Team1               6         ---                          Incompatible
Bld1_Floor_2           2         x930-5.5.2-2.1.rel           Release Ready
Bld1_Floor_1           4         ---                          Incompatible
Building_1             2         ---                          Incompatible
Building_2             2         x950-5.5.2-2.1.rel           Release Ready
Continue upgrading releases ? (y/n):
```

atmf recover

Overview This command is used to manually initiate the recovery (or replication) of an AMF node, usually when a node is being replaced.

Syntax

```
atmf recover [<node-name> master <node-name>]
atmf recover [<node-name> controller <node-name>]
```

Parameter	Description
<node-name>	The name of the device whose configuration is to be recovered or replicated.
`master` *<node-name>*	The name of the master device that holds the required configuration information. 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. Note that although you can omit both the node name and the controller name; you cannot specify a controller name unless you also specify the node name.

Mode Privileged Exec

Usage notes The recovery/replication process involves loading the configuration file for a node that is either about to be replaced or has experienced some problem. You can specify the configuration file of the device being replaced by using the *<node-name>* parameter, and you can specify the name of the master node or controller holding the configuration file.

If the *<node-name>* parameter is not entered then the node will attempt to use one that has been previously configured. If the replacement node has no previous configuration (and has no previously used node-name), then the recovery will fail.

If the master or controller name is not specified then the device will poll all known AMF masters and controllers and execute an election process (based on the last successful backup and its timestamp) to determine which to use. If no valid backup master or controller is found, then this command will fail.

No error checking occurs when this command is run. Regardless of the last backup status, the recovering node will attempt to load its configuration from the specified master node or controller.

If the node has previously been configured, we recommend that you suspend any AMF backup before running this command. This is to prevent corruption of the backup files on the AMF master as it attempts to both backup and recover the node at the same time.

Example To recover the AMF node named Node_10 from the AMF master node named Master_2, use the following command:

```
Master_2# atmf recover Node_10 master Master_2
```

Related commands

atmf backup stop

show atmf backup

show atmf

atmf recover guest

Overview Use this command to initiate a guest node recovery or replacement by reloading its backup file-set that is located within the AMF backup system. Note that this command must be run on the edge node device that connects to the guest node.

Syntax

```
atmf recover guest [<guest-port>]
```

Parameter	Description
<guest-port>	The port number that connects to the guest node.

Mode User Exec/Privileged Exec

Example To recover a guest on node1 port1.0.1, use the following command

```
node1# atmf recover guest port1.0.1
```

Related commands show atmf backup guest

atmf recover led-off

Overview This command turns off the recovery failure flashing port LEDs. It reverts the LED's function to their normal operational mode, and in doing so assists with resolving the recovery problem. You can repeat this process until the recovery failure has been resolved. For more information, see the AMF Feature Overview and Configuration Guide.

Syntax
```
atmf recover led-off
```

Default Normal operational mode

Mode Privileged Exec

Example To revert the LEDs on Node1 from recovery mode display to their normal operational mode, use the command:

```
Node1# atmf recover led-off
```

Related commands atmf recover

atmf recover over-eth

Overview Use this command to enable AMF recovery over an AR-series device's Eth port. This setting persists even after restoring a device to a 'clean' state with the erase factory-default or atmf cleanup command.

Use the **no** variant of this command to disable AMF recover over an Eth port.

Syntax

```
atmf recover over-eth
no atmf recover over-eth
```

Default Eth ports cannot be used for recovery.

Mode Privileged Exec

Usage notes AMF links over Eth ports are only available if your network is running in AMF secure mode (see atmf secure-mode for more information on AMF secure mode).

Example To enable AMF recovery over an Eth port, use the command:

```
awplus# atmf recover over-eth
```

To disable AMF recovery over an Eth port, use the commands:

```
awplus# no atmf recover over-eth
```

Related commands

atmf-link

atmf recover

atmf secure-mode

erase factory-default

show atmf detail

Command changes Version 5.5.0-1.1: command added

atmf recovery-server

Overview Use this command on an AMF master to process recovery requests from isolated AMF nodes. An isolated node is an AMF member that is only connected to the rest of the AMF network via a virtual-link.

This option allows these nodes, which have no AMF neighbors, to be identified for recovery or provisioning purposes. They are identified using an identity token which is stored on the AMF master.

Use the **no** variant of this command to disable processing of recovery requests from isolated AMF nodes.

Syntax

```
atmf recovery-server
no atmf recovery-server
```

Default Recovery-server is disabled by default.

Mode Global Configuration

Usage notes Once **recovery-server** is enabled on an AMF network, the next time an isolated node is backed up its identity token will be stored in the AMF master's database. Should the device fail it can then be replaced and auto-recovery will occur as long as:

- the AMF master is accessible to the isolated node, and
- either, a DHCP server is configured to send the Uniform Resource Identifier (URI) of the AMF master to the recovering node, or
- a DNS server is configured to resolve the default recovery URI (https://amfrecovery.alliedtelesis.com) to the IP address of the AMF master.

Provisioning of isolated nodes is achieved by creating an identity token for the new node using the identity (amf-provision) command.

See the AMF Feature Overview and Configuration Guide for information on preparing your network for recovering or provisioning isolated nodes.

Example To enable recovery-server on an AMF master, use the commands:

```
awplus# configure terminal
awplus(config)# atmf recovery-server
```

To disable recovery-server on an AMF master, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf recovery-server
```

Related commands

atmf backup

atmf cleanup

identity (amf-provision)

atmf virtual-link

Command changes Version 5.4.7-2.1: command added

atmf remote-login

Overview Use this command to remotely login to other AMF nodes in order to run commands as if you were a local user of that node.

Syntax

```
atmf remote-login [user <name>] <nodename>
```

Parameter	Description
<name>	The name of a user on the remote node.
<nodename>	The name of the remote AMF node you are connecting to.

Mode Privileged Exec (This command will only run at privilege level 15)

Usage notes You do not need a valid login on the local device in order to run this command. The session will take you to the enable prompt on the new device. If the remote login session exits for any reason (e.g. device reboot) you will be returned to the originating node.

You can create additional user accounts on nodes. AMF's goal is to provide a uniform management plane across the whole network, so we recommend you use the same user accounts on all the nodes in the network.

In reality, though, it is not essential to have the same accounts on all the nodes. Users can remote login from one node to a second node even if they are logged into the first node with a user account that does not exist on the second node (provided that atmf restricted-login is disabled and the user account on the first node has privilege level 15).

Moreover, it is possible to use a RADIUS or TACACS+ server to manage user authentication, so users can log into AMF nodes using user accounts that are present on the RADIUS or TACACS+ server, and not present in the local user databases of the AMF nodes.

The software will not allow you to run multiple remote login sessions. You must exit an existing session before starting a new one.

If you disconnect from the VTY session without first exiting from the AMF remote session, the device will keep the AMF remote session open until the exec-timeout time expires (10 minutes by default). If the exec-timeout time is set to infinity (**exec-timeout 0 0**), then the device is unable to ever close the remote session. To avoid this, we recommend you use the **exit** command to close AMF remote sessions, instead of closing the associated VTY sessions. We also recommend you avoid setting the exec-timeout to infinity.

Example To remotely login from node Node10 to Node20, use the following command:

```
Node10# atmf remote-login node20
Node20>
```

To close the session on Node20 and return to Node10's command line, use the following command:

```
Node20# exit
Node10#
```

In this example, user User1 is a valid user of node5. They can remotely login from node5 to node3 by using the following commands:

```
node5# atmf remote-login user User1 node3
node3> enable
```

Related commands atmf restricted-login

Command changes Version 5.4.6-2.1: changes to AMF user account requirements

atmf restricted-login

Overview By default, users who are logged into any node on an AMF network are able to manage any other node by using either working-sets or an AMF remote login. If the access provided by this feature is too wide, or contravenes network security restrictions, it can be limited by running this command, which changes the access so that:

- users who are logged into non-master nodes cannot execute any commands that involve working-sets, and
- from non-master nodes, users can use remote-login, but only to login to a user account that is valid on the remote device (via a statically configured account or RADIUS/TACACS+). Users are also required to enter the password for that user account.

Once entered on any AMF master node, this command will propagate across the network.

Use the **no** variant of this command to disable restricted login on the AMF network. This allows access to the **atmf working-set** command from any node in the AMF network.

Syntax

```
atmf restricted-login
no atmf restricted-login
```

Mode Privileged Exec

Default Master nodes operate with **atmf restricted-login** disabled.

Member nodes operate with **atmf restricted-login** enabled.

NOTE: *The default conditions of this command vary from those applied by its "no" variant. This is because the restricted-login action is only applied by **master** nodes, and in the absence of a master node, the default is to apply the restricted action to all **member** nodes with AMF configured.*

Usage notes In the presence of a **master** node, its default of **atmf restricted-login disabled** will propagate to all its member nodes. Similarly, any change in this command's status that is made on a master node, will also propagate to all its member nodes

Note that once you have run this command, certain other commands that utilize the AMF working-set command, such as the **include**, **atmf reboot-rolling** and **show atmf group members** commands, will operate only on master nodes.

Restricted-login must be enabled on AMF areas with more than 120 nodes.

Example To enable restricted login, use the command

```
Node_20(config)# atmf restricted-login node20
```

Related commands atmf remote-login

show atmf

Command changes Version 5.4.6-2.1: changes to AMF user account requirements

atmf retry guest-link

Overview Use this command to retry an AMF guest-link by restarting AMF guest discovery on a port if it is currently in the failed state.

If no port is specified then all configured AMF guest-link ports that are in the failed state are retried.

If a port is specified then that port will only be retried if it is both:

- configured as an AMF guest-link, and
- it is currently in the failed state.

Syntax

```
atmf retry guest-link [<interface>]
```

Parameter	Description
<interface>	Name of the interface the guest-link you want to retry is configured on.

Mode Privileged Exec

Example To retry all configured AMF guest-link currently in a failed state, use the command:

```
awplus# atmf retry guest-link
```

To retry an AMF guest-link configured on port1.0.2 currently in a failed state, use the command:

```
awplus# atmf retry guest-link port1.0.2
```

Related commands show atmf links guest

switchport atmf-guestlink

atmf secure-mode

Overview Use this command to enable AMF secure mode on an AMF node. AMF secure mode makes an AMF network more secure by:

- Adding an authorization mechanism before and AMF member is allowed to join an AMF network.
- The encryption of all AMF packets sent between AMF nodes.
- Adding support for user login authentication by RADIUS or TACACS+, and removing the requirement to have the same privileged user account in the local user database on all devices in the AMF network.
- Adding additional logging which enables network administrators to monitor attempts to gain unauthorized access to the AMF network.

Once the secure mode command is run on all nodes on an AMF network, the AMF masters and AMF controllers manage the addition of AMF nodes and AMF areas to the AMF network.

Use the **no** variant of this command to disable AMF secure mode on an AMF node.

Syntax

```
atmf secure-mode
no atmf secure-mode
```

Default Secure mode is disabled by default.

Mode Global Configuration

Usage notes When an AMF network is running in AMF secure mode the atmf restricted-login feature is automatically enabled. This restricts the atmf working-set command to users that are logged on to an AMF master. This feature cannot be disabled independently of secure mode.

When AMF secure mode is enabled the AMF controllers and masters in the AMF network form a group of certificate authorities. A node may only join a secure AMF network once it has been authorized by a master or controller. When enabled, all devices in the AMF network must be running in secure mode. Unsecured devices will not be able to join a secure AMF network.

Example To enable AMF secure mode on an AMF node, use the commands:

```
awplus# configure terminal
awplus(config)# atmf secure-mode
```

To disable AMF secure mode on an AMF node, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf secure-mode
```

Related commands atmf authorize

atmf secure-mode certificate expiry

clear atmf secure-mode certificates

clear atmf secure-mode statistics

show atmf

show atmf authorization

show atmf secure-mode

show atmf secure-mode certificates

show atmf secure-mode sa

show atmf secure-mode statistics

Command changes Version 5.4.7-0.3: command added

atmf secure-mode certificate expire

Overview Use this command on an AMF master to expire a secure mode certificate. Running this command will force the removal of the AMF node from the network.

Syntax
```
atmf secure-mode certificate expire <node-name> [area
<area-name>]
```

Parameter	Description
<node-name>	Name of the AMF node you want to expire the certificate for.
area	Specify an AMF area.
<area-name>	Name of the AMF area you want to expire the AMF nodes certificate for.

Mode Privileged Exec

Example To remove an AMF node named “node3” from an AMF network, use the following command on the AMF master:

```
awplus# atmf secure-mode certificate expire node3
```

To remove an AMF node named “node2” in an area named “area2”, use the following command on the AMF master:

```
awplus# atmf secure-mode certificate expire node2 area area2
```

Related commands
atmf secure-mode

show atmf secure-mode

show atmf secure-mode certificates

Command changes Version 5.4.7-0.3: command added

atmf secure-mode certificate expiry

Overview Use this command to set the expiry time of AMF secure mode certificates. Once an AMF node's certificate expires it must re-authorize and obtain a new certificate from the AMF master.

Use the **no** variant of this command to reset the expiry time to 180 days.

Syntax

```
atmf secure-mode certificate expiry {<days>|infinite}
no atmf secure-mode certificate expiry
```

Parameter	Description
<days>	Length of time, in days, that an AMF secure mode certificate remains valid. A value between 1 and 365.
infinite	The authorization certificate does not expire, in other words AMF nodes stay authorized indefinitely.

Default The default expiry time is 180 days.

Mode Global Configuration

Example To set AMF secure mode certificate expiry to 7 days, use the commands:

```
awplus# configure terminal
awplus(config)# atmf secure-mode certificate expiry 7
```

To set AMF secure mode certificates to never expire, use the commands:

```
awplus# configure terminal
awplus(config)# atmf secure-mode certificate expiry infinite
```

To reset the certificate expiry to 180 days, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf secure-mode certificate expiry
```

Related commands atmf secure-mode

show atmf secure-mode

show atmf secure-mode certificates

Command changes Version 5.4.7-0.3: command added

atmf secure-mode certificate renew

Overview Use this command to force all local certificates to expire and be renewed on an AMF secure mode network.

Secure mode certificates renew automatically but this command could be used to renew a certificate in a situation where the automatic renewal may happen while the device is not attached to the AMF network.

Syntax
```
atmf secure-mode certificate renew
```

Mode Privileged Exec

Example To renew a local certificate on a AMF member or AMF master, use the command:

```
awplus# atmf secure-mode certificate renew
```

Related commands show atmf secure-mode certificates

show atmf secure-mode statistics

Command changes Version 5.4.7-0.3: command added

atmf secure-mode enable-all

Overview Use this command to enable AMF secure mode on an entire network. AMF secure mode makes an AMF network more secure by:

- Adding an authorization mechanism before an AMF member is allowed to join an AMF network.
- The encryption of all AMF packets sent between AMF nodes.
- Adding support for user login authentication by RADIUS or TACACS+, and removing the requirement to have the same privileged user account in the local user database on all devices in the AMF network.
- Adding additional logging which enables network administrators to monitor attempts to gain unauthorized access to the AMF network.

Once this command is run on an AMF network, the AMF masters and AMF controllers manage the addition of AMF nodes and AMF areas to the AMF network.

This command can only be run on an AMF master.

Use the **no** variant of this command to disable AMF secure mode on an entire network.

Syntax

```
atmf secure-mode enable-all
no atmf secure-mode enable-all
```

Default Secure mode is disabled by default.

Mode Privileged Exec

Usage notes When an AMF network is running in AMF secure mode the atmf restricted-login feature is automatically enabled. This restricts the atmf working-set command to users that are logged on to an AMF master. This feature cannot be disabled independently of secure mode.

When AMF secure mode is enabled the AMF controllers and masters in the AMF network form a group of certificate authorities. A node may only join a secure AMF network once it has been authorized by a master or controller. When enabled, all devices in the AMF network must be running in secure mode. Unsecured devices will not be able to join a secure AMF network.

Running **atmf secure-mode enable-all**:

- Groups all AMF members in a working set.
- Executes clear atmf secure-mode certificates on the working set of members, which removes existing secure mode certificates from all the nodes.
- Groups all the AMF masters in a working set.
- Executes atmf authorize provision **all** on the working set of masters, so all masters provision all nodes.
- Groups all AMF nodes in a working set.

- Runs a script which executes atmf secure-mode and then writes the configuration file on each node.
- Starts a timer that ticks every 10 seconds, for a maximum of 10 times, and checks if all the secure mode capable nodes rejoin the AMF network.

Running **no atmf secure-mode enable-all**:

- Groups all AMF nodes in a working set.
- Runs a script which executes **no** atmf secure-mode and then writes the configuration file on each node.
- Starts a timer that ticks every 10 seconds, for a maximum of 10 times, and checks if all the secure mode capable nodes rejoin the AMF network.

NOTE: *Enabling or disabling secure mode on the network saves the running-config on every device.*

Example To enable AMF secure mode on the entire network, use the command:

```
awplus# atmf secure-mode enable-all
```

You will be prompted to confirm the action:

```
Total number of nodes 21
21 nodes support secure-mode

Enable secure-mode across the AMF network ? (y/n): y
```

To disable AMF secure mode on the entire network, use the command:

```
awplus# no atmf secure-mode enable-all
```

You will be prompted to confirm the action:

```
% Warning: All security certificates will be deleted.
Disable secure-mode across the AMF network ? (y/n): y
```

Related commands show atmf

Command changes Version 5.4.7-0.3: command added

atmf select-area

Overview Use this command to access devices in an area outside the core area on the controller network. This command will connect you to the remote area-master of the specified area.

This command is only valid on AMF controllers.

The **no** variant of this command disconnects you from the remote area-master.

Syntax

```
atmf select-area {<area-name>|local}
no atmf select-area
```

Parameter	Description
<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 notes After running this command, use the atmf working-set command to select the set of nodes you want to access in the remote area.

Example To access nodes in the area Canterbury, use the command

```
controller-1# atmf select-area Canterbury
```

This displays the following output:

```
Test_network[3]#atmf select-area Canterbury
=============================================
Connected to area Canterbury via host Avensis:
=============================================
```

To return to the local area for controller-1, use the command

```
controller-1# atmf select-area local
```

Alternatively, to return to the local area for controller-1, use the command

```
controller-1# no atmf select-area
```

Related commands atmf working-set

atmf topology-gui enable

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

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

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

Syntax

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

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

Mode Global Configuration mode

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

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

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

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

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

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

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

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

Related commands atmf enable

log event-host

service http

atmf trustpoint

Overview Use this command to set a PKI trustpoint for an AMF network. This command needs to be run on an AMF master or controller.

The self-signed certificate authority (CA) certificate is distributed to every node on the AMF network. It is used to verify client certificates signed by the trustpoint.

Use the **no** variant of this command to remove an AMF trustpoint.

Syntax

```
atmf trustpoint <trustpoint-name>
no atmf trustpoint <trustpoint-name>
```

Parameter	Description
<trustpoint-name>	Name of the trustpoint.

Default No trustpoint is configured by default.

Mode Global Configuration

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

Create a self-signed trustpoint called 'our_trustpoint' with keypair 'our_key':

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

Create the root and server certificates for this trustpoint:

```
awplus# crypto pki authenticate our_trustpoint
awplus# crypto pki enroll our_trustpoint
```

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

Example To configure an AMF trustpoint for the trustpoint 'our_trustpoint', use the commands:

```
awplus# configure terminal
awplus(config)# atmf trustpoint our_trustpoint
```

To remove an AMF trustpoint for the trustpoint 'our_trustpoint', use the commands:

```
awplus# configure terminal
awplus(config)# no atmf trustpoint our_trustpoint
```

Related commands

crypto pki trustpoint

show atmf

Command changes

Version 5.4.7-2.1: command added

atmf virtual-crosslink

Overview Use this command to create a virtual crosslink. A virtual crosslink connects an AMF master or controller on a physical device to a Virtual AMF Appliance (VAA) master or controller.

All AMF master nodes must reside in the same AMF domain and are required to be directly connected using AMF crosslinks. In order to be able to meet this requirement for AMF masters running on VAAs, a virtual crosslink connects the AMF master or controller on the physical device to the master or controller on the VAA.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove a virtual crosslink.

Syntax

```
atmf virtual-crosslink id <local-id> ip <local-ip> remote-id
<remote-id> remote-ip <remote-ip>
```

```
atmf virtual-crosslink id <local-id> ip <local-ip> remote-id
<remote-id> remote-host <domainname>
```

```
no atmf virtual-crosslink id <local-id>
```

Parameter	Description
`id <local-id>`	ID of the local tunnel port, a value between 1 and 4094.
`ip <local-ip>`	IPv4 address of the local tunnel port in a.b.c.d format.
`remote-id <remote-id>`	ID of the remote tunnel port, a value between 1 and 4094.
`remote-ip <remote-ip>`	IPv4 address of the remote tunnel port in a.b.c.d format.
`remote-host <domainname>`	The domain name of the remote node.

Default No AMF virtual crosslinks are created by default.

Mode Global Configuration

Usage notes This command allows a virtual tunnel to be created between two remote sites over a Layer 3 link. The tunnel encapsulates AMF packets and allows them to be sent transparently across a Wide Area Network (WAN) such as the Internet.

Configuration involves creating a local tunnel ID, a local IP address, a remote tunnel ID, and a remote IP address or domain name. Each side of the tunnel must be configured with the same, but mirrored parameters.

NOTE: *Virtual crosslinks are not supported on AMF container masters, therefore if multiple tenants on a single VAA host are configured for secure mode, only a single AMF master is supported per area.*

Example To setup a virtual link from a local site, 'siteA', to a remote site, 'siteB', (assuming there is already IP connectivity between the sites), run the following commands at the local site:

```
siteA# configure terminal
siteA(config)# atmf virtual-crosslink id 5 ip 192.168.100.1
remote-id 10 remote-ip 192.168.200.1
```

At the remote site, run the commands:

```
siteB# configure terminal
siteB(config)# atmf virtual-crosslink id 10 ip 192.168.200.1
remote-id 5 remote-ip 192.168.100.1
```

To remove this virtual crosslink, run the following commands on the local site:

```
siteA# configure terminal
siteA(config)# no atmf virtual-crosslink id 5
```

On the remote site, run the commands:

```
siteB# configure terminal
siteB(config)# no atmf virtual-crosslink id 10
```

Related commands

atmf virtual-crosslink

show atmf links

switchport atmf-crosslink

Command changes

Version 5.5.2-0.1: **remote-host** parameter added

Version 5.4.7-0.3: command added

atmf virtual-link

Overview This command creates one or more Layer 2 tunnels that enable AMF nodes to transparently communicate across a wide area network using Layer 2 connectivity protocols.

Once connected through the tunnel, the remote member will have the same AMF capabilities as a directly connected AMF member.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove the specified virtual link.

Syntax

```
atmf virtual-link id <1-4094> ip <a.b.c.d> remote-id <1-4094>
remote-ip <a.b.c.d> [remote-area <area-name>]

atmf virtual-link id <1-4094> interface <interface-name>
remote-id <1-4094> remote-ip <a.b.c.d> [remote-area
<area-name>]

atmf virtual-link id <1-4094> ip <a.b.c.d> remote-id <1-4094>
remote-host <domainname> [remote-area <area-name>]

atmf virtual-link id <1-4094> interface <interface-name>
remote-id <1-4094> remote-host <domainname> [remote-area
<area-name>]

no atmf virtual-link id <1-4094>
```

Parameter	Description
`id <1-4094>`	ID of the local tunnel point, in the range 1 to 4094.
`ip <a.b.c.d>`	Specify the local IP address of the local interface for the virtual-link (alternatively you can specify the interface's name, see below).
`interface <interface-name>`	Specify the local interface name for the virtual-link. This allows you to use a dynamic, rather than a static, local IP address.
`remote-id <1-4094>`	The ID of the (same) tunnel that will be applied by the remote node. Note that this must match the local-id that is defined on the remote node. This means that (for the same tunnel) the local and remote tunnel IDs are reversed on the local and remote nodes.
`remote-ip <a.b.c.d>`	The IP address of the remote node.
`remote-host <domainname>`	The domain name of the remote node.
`remote-area <area-name>`	The name of the remote area connected to this virtual-link.

Mode Global Configuration

Usage notes The Layer 2 tunnel that this command creates enables a local AMF session to appear to pass transparently across a Wide Area Network (WAN) such as the Internet. The addresses configured as the local and remote tunnel IP addresses must have IP connectivity to each other. If the tunnel is configured to connect a head office and branch office over the Internet, typically this would involve using some type of managed WAN service such as a site-to-site VPN. Tunnels are only supported using IPv4.

Configuration involves creating a local tunnel ID, a local IP address, a remote tunnel ID and a remote IP address or domain name. A reciprocal configuration is also required on the corresponding remote device. The local tunnel ID must be unique to the device on which it is configured.

If an interface acquires its IP address dynamically then the local side of the tunnel can be specified by using the interface's name instead of using its IP address. When using a dynamic local address the remote address of the other side of the virtual-link must be configured with either:

- the IP address of the NAT device the dynamically configured interface is behind, or
- 0.0.0.0, if the virtual-link is configured as a secure virtual-link.

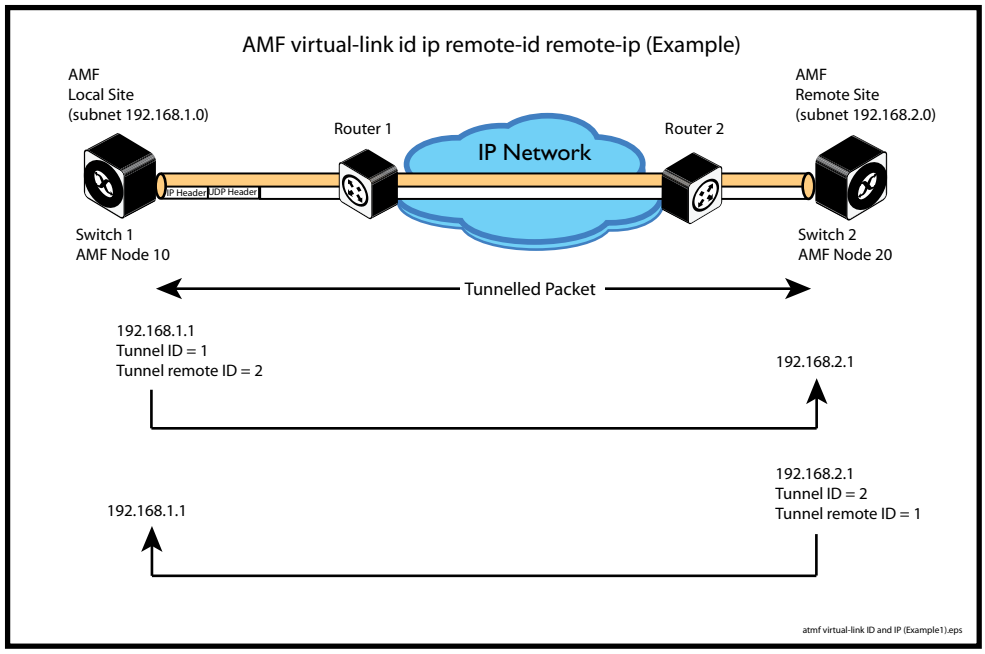
For instructions on how to configure dynamic IP addresses on virtual-links, see the AMF Feature Overview and Configuration Guide.

The tunneled link may operate via external (non AlliedWare Plus) routers in order to provide wide area network connectivity. However in this configuration, the routers perform a conventional router to router connection. The protocol tunneling function is accomplished by the AMF nodes.

NOTE: *AMF cannot achieve zero touch replacement of the remote device that terminates the tunnel connection, because you must pre-configure the local IP address and tunnel ID on that remote device.*

Example 1 Use the following commands to create the tunnel shown in the figure below.

Figure 21-2: AMF virtual link example




```
Node_10(config)# atmf virtual-link id 1 ip 192.168.1.1
remote-id 2 remote-ip 192.168.2.1
```

```
Node_20(config)# atmf virtual-link id 2 ip 192.168.2.1
remote-id 1 remote-ip 192.168.1.1
```

Example 2 To set up an area virtual link to a remote site (assuming IP connectivity between the sites already), one site must run the following commands:

```
SiteA# configure terminal
```

```
SiteA(config)# atmf virtual-link id 5 ip 192.168.100.1
remote-id 10 remote-ip 192.168.200.1 remote-area SiteB-AREA
```

The second site must run the following commands:

```
SiteB# configure terminal
```

```
SiteB(config)# atmf virtual-link id 10 ip 192.168.200.1
remote-id 5 remote-ip 192.168.100.1 remote-area SiteA-AREA
```

Before you can apply the above **atmf virtual-link** command, you must configure the area names *SiteB-AREA* and *SiteA-AREA*.

Related commands

atmf virtual-link description

atmf virtual-link protection

show atmf

show atmf links

show atmf virtual-links

Command changes

Version 5.5.2-0.1: **remote-host** parameter added

Version 5.4.9-0.1: **interface** parameter added

atmf virtual-link description

Overview Use this command to add a description to an existing AMF virtual-link.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove a description from an AMF virtual-link.

Syntax

```
atmf virtual-link id <1-4094> description <description>
no atmf virtual-link id <1-4094> description
```

Parameter	Description
`id <1-4094>`	ID of the local tunnel point.
`<description>`	A description for the virtual-link.

Default No description is set by default.

Mode Global Configuration

Example To add a description to the virtual-link with id '5', use the commands:

```
awplus# configure terminal
awplus(config)# atmf virtual-link id 5 description TO SITE B
```

To remove a description from the virtual-link with id '5', use the commands:

```
awplus# configure terminal
awplus(config)# no atmf virtual-link id 5
```

Related commands

atmf virtual-link

show atmf links

show atmf virtual-links

atmf virtual-link protection

Overview Use this command to add protection to an existing AMF virtual-link. Secure AMF virtual-links encapsulate the L2TPv3 frames of the virtual-link with IPsec.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove protection from an AMF virtual-link.

Syntax

```
atmf virtual-link id <1-4094> protection ipsec key [8]
<key-string>
```

```
no atmf virtual-link id <1-4094> protection
```

Parameter	Description
`id`	Specify the link ID.
<1-4094>	Link ID in the range 1 to 4094
`protection`	Protection is on for this link.
`ipsec`	Security provided using IPsec.
`key`	Set the shared key.
`8`	Specifies a string in an encrypted format instead of plain text. The running config will display the new password as an encrypted string even if password encryption is turned off.
<key-string>	Specify the shared key for the link.

Default Protection is off by default.

Mode Global Configuration

Usage notes Considered the following limitations when creating a secure virtual-link:

- Switch devices support a maximum of 20 downstream AMF nodes when using a secure virtual-link as an uplink.
- When there are two or more AMF members behind a shared NAT device, only one of the members will be able to use secure virtual-links.
- An AMF multi-tenant environment supports a maximum cumulative total of 1200 secure virtual-links across all AMF containers.

Example To create and configure a virtual link with protection, first create the virtual-link:

```
Host-A# configure terminal
```

```
Host-A(config)# atmf virtual-link id 1 ip 192.168.1.1 remote-id
2 remote-ip 192.168.2.1
```

The enable protection on the virtual link:

```
Host-A(config)# atmf virtual-link id 1 protection ipsec key
securepassword
```

Repeat these steps on the other side of the link:

```
Host-B(config)# atmf virtual-link id 2 ip 192.168.2.1 remote-id
1 remote-ip 192.168.1.1
```

```
Host-B(config)# atmf virtual-link id 2 protection ipsec key
securepassword
```

Related commands

atmf virtual-link

show atmf

show atmf links

show atmf virtual-links

Command changes

Version 5.4.9-0.1: command added

atmf working-set

Overview Use this command to execute commands across an individually listed set of AMF nodes or across a named group of nodes.

Note that this command can only be run on a master node.

Use the **no** variant of this command to remove members or groups from the current working-set.

Syntax

```
atmf working-set {[<node-list>]|[group
{<group-list>|all|local|current}]}
```

```
no atmf working-set {[<node-list>]|[group <group-list>]}
```

Parameter	Description
<node-list>	A comma delimited list (without spaces) of nodes to be included in the working-set.
`group`	The AMF group.
<group-list>	A comma delimited list (without spaces) of groups to be included in the working-set. Note that this can include either defined groups, or any of the Automatic, or Implicit Groups shown earlier in the bulleted list of groups.
`all`	All nodes in the AMF.
`local`	Local node Running this command with the parameters **group local** will return you to the local prompt and local node connectivity.
`current`	Nodes in current list.

Mode Privileged Exec

Usage notes You can put AMF nodes into groups by using the atmf group (membership) command.

This command opens a session on multiple network devices. When you change the working set to anything other than the local device, the prompt will change to the AMF network name, followed by the size of the working set, shown in square brackets. This command has to be run at privilege level 15.

In addition to the user defined groups, the following system assigned groups are automatically created:

- Implicit Groups
  - local: The originating node.
  - current: All nodes that comprise the current working-set.
  - all: All nodes in the AMF.

- Automatic Groups - These can be defined by hardware architecture, e.g. x510, x610, x8100, AR3050S or AR4050S, or by certain AMF nodal designations such as master.

Note that the Implicit Groups do not appear in show atmf group command output.

If a node is an AMF master it will be automatically added to the master group.

Example 1 To add all nodes in the AMF to the working-set, use the command:

```
node1# 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 connect to only the local node, use the command:

```
ATMF_Network_Name[6]# atmf working-set group local
node1#
```

The following table describes the meaning of the prompts in this example.

Parameter	Description
ATMF_Network_Name	The name of the AMF network, as set by the atmf network-name command.
[6]	The number of nodes in the working-set.
node1	The name of the local node, as set by the hostname command.

bridge-group (amf-container)

Overview Use this command to connect an AMF container to a bridge created on a Virtual AMF Appliance (VAA) virtual machine for AMF Cloud. This allows the AMF container to connect to a physical network.

Note that this command is only available on AMF Cloud, not on AlliedWare Plus switches.

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the AMF Feature Overview and Configuration Guide for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove a bridge-group from an AMF container.

Syntax

```
bridge-group <bridge-id>
no bridge-group
```

Parameter	Description
<bridge-id>	The ID of the bridge group to join, a number between 1 and 64.

Mode AMF Container Configuration

Usage notes Each container has two virtual interfaces:

1) Interface eth0, used to connect to the AMF controller on the VAA host via an AMF area-link, and configured using this area-link command.

2) Interface eth1, used to connect to the outside world using a bridged L2 network link, and configured using the **bridge-group** command.

Before using this command, a bridge must be created with the same bridge-id on the VAA host using the **bridge <bridge-id>** command.

See the AMF Feature Overview and Configuration Guide for more information on configuring the bridge.

Example To assign a bridge group to AMF container 'vac-wlg-1', use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# bridge-group 1
```

Related commands

atmf container

show atmf container

Command changes Version 5.4.7-0.1: command added

clear application-proxy threat-protection

Overview Use this command to clear the threat protection for a specified address.

Syntax

```
clear application-proxy threat-protection {<ip-address>|
<mac-address>|all}
```

Parameter	Description
`<ip-address>`	The IPv4 address you wish to clear the threat for, in A.B.C.D format.
`<mac-address>`	The MAC address you wish to clear the threat for, in HHHH.HHHH.HHHH format.
`all`	Clear the threat for all IPv4 and MAC addresses.

Mode Privileged Exec

Example To clear the threat for 10.34.199.117, use the command:

```
awplus# clear application-proxy threat-protection 10.34.199.117
```

Related commands

application-proxy quarantine-vlan

application-proxy threat-protection

application-proxy threat-protection send-summary

service atmf-application-proxy

show application-proxy threat-protection

Command changes Version 5.4.7-2.2: command added

clear atmf links

Overview Use this command with no parameters to manually reset all the AMF links on a device. You can optionally specify an interface or range of interfaces to reset the links on.

Certain events or topology changes can cause AMF links to be incorrect or outdated. Clearing the links forces AMF to relearn the information from neighboring nodes and create a fresh, correct, view of the network.

Syntax

```
clear atmf links [<interface-list>]
```

Parameter	Description
<interface-list>	The interfaces or ports to perform the reset on. An interface-list can be: • a switchport (e.g. port1.0.1) • a static channel group (e.g. sa2) • a dynamic (LACP) channel group (e.g. po2) • a local port (e.g. of0) • You can specify a continuous range of interfaces separated by a hyphen, or a comma-separated list (e.g. port1.0.1, port1.0.4-port1.0.18). The specified interfaces must exist. If this parameter is left out then all links of the specified type will be reset on the device.

Mode Privileged Exec

Example To clear all AMF links on a device, use the following command:

```
awplus# clear atmf links
```

To clear all AMF links on port1.0.1 to port1.0.4 and static aggregator sa1, use the following command:

```
awplus# clear atmf links port1.0.1-port1.0.4,sa1
```

Related commands clear atmf links virtual

show atmf links

Command changes Version 5.4.8-2.1: command added

clear atmf links virtual

Overview Use this command with no parameters to manually reset all the AMF virtual links on a device. You can, optionally, specify a comma separated list of virtual links to reset.

Certain events or topology changes can cause AMF links to be incorrect or outdated. Clearing the links forces AMF to relearn the information from neighboring nodes and create a fresh, correct view of the network.

Syntax

```
clear atmf links virtual [<virtuallink-list>]
```

Parameter	Description
<virtuallink-list>	A single, or list, of AMF virtual link identifiers to reset. This must be a comma separated list of links e.g. *vlink1, vlink2, vlink3*. Specifying a link range e.g *vlink1-vlink3* is not supported.

Mode Privileged Exec

Example To clear all AMF virtual links on a device, use the following command:

```
awplus# clear atmf links virtual
```

To clear AMF virtual links vlink11 and vlink21, use the following command:

```
awplus# clear atmf links virtual vlink11,vlink22
```

Related commands clear atmf links

show atmf links

Command changes Version 5.4.8-2.1: command added

clear atmf links statistics

Overview This command resets the values of all AMF link, port, and global statistics to zero.

Syntax
```
clear atmf links statistics
```

Mode Privilege Exec

Example To reset the AMF link statistics values, use the command:

```
node_1# clear atmf links statistics
```

Related commands show atmf links statistics

clear atmf recovery-file

Overview Use this command to delete all of a node's recovery files. It deletes the recovery files stored on:

- the local node,
- neighbor nodes, and
- external media (USB or SD card).

Syntax

```
clear atmf recovery-file
```

Mode Privileged Exec

Usage notes AMF recovery files are created for nodes with special links. Special links include:

- virtual links,
- area links terminating on an AMF master, and
- area virtual links terminating on an AMF master.

An AMF node with one of these special links pushes its startup configuration to its neighbors and to any attached external media. It then fetches and applies this configuration at recovery time. This configuration enables it to contact the AMF master and initiate a recovery.

Recovery files can become out of date if:

- a node's neighbor is off line when changes are made to its configuration, or
- when a node no longer contains a special link.

Example To clear a node's recovery files, use the command:

```
node1# clear atmf recovery-file
```

Output Figure 21-3: If AlliedWare Plus detects that a node contains a special link then the following message is displayed

```
node1#clear atmf recovery-file
% Warning: ATMF recovery files have been removed.
ATMF recovery may fail. Please save running-configuration.
```

Related commands show atmf recovery-file

Command changes Version 5.4.8-0.2: command added

clear atmf secure-mode certificates

Overview Use this command to remove all certificates from an AMF member or master. AMF nodes will need to be re-authorized once this command has been run.

Syntax

```
clear atmf secure-mode certificates
```

Mode Privileged Exec

Example To clear all certificates from an AMF node, use the command:

```
awplus# clear atmf secure-mode certificates
```

If this is the only master on the network you will see the following warning:

```
% Warning: This node is the only master in the network!
All the nodes will become isolated and refuse to join any ATMF
network. The certificates on all the isolated nodes must be
cleared before rejoining an ATMF network will be possible.

To clear certificates a reboot of the device is required.
Clear certificates and Reboot ? (y/n):
```

On an AMF member you will see the following message:

```
To clear certificates a reboot of the device is required.
Clear certificates and Reboot ? (y/n):
```

Related commands

atmf authorize

atmf secure-mode

show atmf authorization

show atmf secure-mode certificates

Command changes Version 5.4.7-0.3: command added

clear atmf secure-mode statistics

Overview Use this command to reset all secure mode statistics to 0.

Syntax
```
clear atmf secure-mode statistics
```

Mode Privileged Exec

Example To reset the AMF secure mode statistics information, use the command:
```
awplus# clear atmf secure-mode statistic
```

Related commands show atmf secure-mode

show atmf secure-mode statistics

Command changes Version 5.4.7-0.3: command added

clone (amf-provision)

Overview This command sets up a space on the backup media for use with a provisioned node and copies into it almost all files and directories from a chosen backup or provisioned node.

Alternatively, you can set up a new, unique provisioned node by using the command create (amf-provision).

Syntax

```
clone <source-nodename>
```

Parameter	Description
<source-nodename>	The name of the node whose configuration is to be copied for loading to the clone.

Mode AMF Provisioning

Usage notes This command is only available on master nodes in the AMF network.

When using this command it is important to be aware of the following:

- A copy of <*media*>:atmf/<*atmf_name*>/nodes/<*source_node*>/flash will be made for the provisioned node and stored in the backup media.
- The directory <*node_backup_dir*>/flash/.config/ssh is excluded from the copy.
- All contents of <*root_backup_dir*>/nodes/<*nodename*> will be deleted or overwritten.
- Settings for the expected location of other provisioned nodes are excluded from the copy.

The active and backup configuration files are automatically modified in the following ways:

- The **hostname** command is modified to match the name of the provisioned node.
- The **stack virtual-chassis-id** command is removed, if present.

Example To copy from the backup of 'device2' to create backup files for the new provisioned node 'device3' use the following command:

```
device1# atmf provision node device3
device1(atmf-provision)# clone device2
```

Figure 21-4: Sample output from the **clone** command

```
device1# atmf provision node device3
device1(atmf-provision)#clone device2
Copying...
Successful operation
```

To confirm that a new provisioned node has been cloned, use the command:

```
device1# show atmf backup
```

The output from this command is shown in the following figure, and shows the details of the new provisioned node 'device3'.

Figure 21-5: Sample output from the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 01 Oct 2018 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7297.0MB)
Server Config .........
  Synchronization ..... Unsynchronized
    Last Run .......... -
   1 .................. Unconfigured
   2 .................. Unconfigured
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

-----------------------------------------------------------------
Node Name     Date          Time      In ATMF  On Media  Status
-----------------------------------------------------------------
device3       -             -         No       Yes       Prov
device1       30 Sep 2018   00:05:49  No       Yes       Good
device2       30 Sep 2018   00:05:44  Yes      Yes       Good
```

Related commands

atmf provision (interface)

atmf provision node

configure boot config (amf-provision)

configure boot system (amf-provision)

copy (amf-provision)

create (amf-provision)

delete (amf-provision)

identity (amf-provision)

license-cert (amf-provision)

locate (amf-provision)

show atmf provision nodes

Command changes

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

configure boot config (amf-provision)

Overview This command sets the configuration file to use during the next boot cycle. This command can also set a backup configuration file to use if the main configuration file cannot be accessed for an AMF provisioned node. To unset the boot configuration or the backup boot configuration use the **no boot** command.

Syntax

```
configure boot config [backup] <file-path|URL>
configure no boot config [backup]
```

Parameter	Description
`backup`	Specify that this is the backup configuration file.
<file-path|URL>	The path or URL and name of the configuration file.

Default No boot configuration files or backup configuration files are specified for the provisioned node.

Mode AMF Provisioning

Usage notes When using this command to set a backup configuration file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

Examples To set the configuration file 'branch.cfg' on the AMF provisioned node 'node1', use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure boot config
branch.cfg
```

To set the configuration file 'backup.cfg' as the backup to the main configuration file on the AMF provisioned node 'node1', use the command:

```
MasterNodeName(atmf-provision)# configure boot config backup
usb:/atmf/amf_net/nodes/node1/config/backup.cfg
```

To unset the boot configuration, use the command:

```
MasterNodeName(atmf-provision)# configure no boot config
```

To unset the backup boot configuration, use the command:

```
MasterNodeName(atmf-provision)# configure no boot config backup
```

Related commands

atmf provision (interface)

atmf provision node

clone (amf-provision)

configure boot system (amf-provision)

create (amf-provision)

delete (amf-provision)

identity (amf-provision)

license-cert (amf-provision)

locate (amf-provision)

show atmf provision nodes

Command changes Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

configure boot system (amf-provision)

Overview This command sets the release file that will load onto a specified provisioned node during the next boot cycle. This command can also set the backup release file to be loaded for an AMF provisioned node. To unset the boot system release file or the backup boot release file use the **no boot** command.

Use the **no** variant of this command to return to the default.

This command can only be run on AMF master nodes.

Syntax

```
configure boot system [backup] <file-path|URL>
configure no boot system [backup]
```

Parameter	Description
<file-path|URL>	The path or URL and name of the release file.

Default No boot release file or backup release files are specified for the provisioned node.

Mode AMF Provisioning

Usage notes When using this command to set a backup release file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

Examples To set the release file x930-5.4.9-0.1.rel on the AMF provisioned node 'node1', use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure boot system
x930-5.4.9-0.1.rel
```

To set the backup release file x930-5.4.8-2.5.rel as the backup to the main release file on the AMF provisioned node 'node1', use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure boot system backup
card:/atmf/amf_net/nodes/node1/flash/x930-5.4.8-2.5.rel
```

To unset the boot release, use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure no boot system
```

To unset the backup boot release, use the command:

```
MasterNodeName# atmf provision node node1
MasterNodeName(atmf-provision)# configure no boot system backup
```

Related commands atmf provision (interface)

atmf provision node

clone (amf-provision)

configure boot config (amf-provision)

create (amf-provision)

delete (amf-provision)

identity (amf-provision)

license-cert (amf-provision)

locate (amf-provision)

show atmf provision nodes

Command changes Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

copy (amf-provision)

Overview Use this command to copy configuration and release files for the node you are provisioning.

For more information about using the copy command see copy (filename) in the File and Configuration Management chapter.

Syntax

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

Parameter	Description
`force`	This parameter forces the copy command to overwrite the destination file, if it already exists, without prompting the user for confirmation.
<source-name>	The filename and path of the source file. See the Introduction of the File and Configuration Management chapter for valid syntax.
<destination-name>	The filename and path for the destination file. See Introduction of the File and Configuration Management chapter for valid syntax.

Mode AMF Provisioning

Example To copy a configuration file named current.cfg from Node_4's Flash into the future_node directory, and set that configuration file to load onto future_node, use the following commands:

```
node_4# atmf provision node future_node
node_4(atmf-provision)# create
node_4(atmf-provision)# locate
node_4(atmf-provision)# copy flash:current.cfg
./future_node.cfg
node_4(atmf-provision)# configure boot config future_node.cfg
```

Related commands

atmf provision (interface)

atmf provision node

clone (amf-provision)

create (amf-provision)

delete (amf-provision)

locate (amf-provision)

show atmf provision nodes

Command changes Version 5.4.9-2.1: command added

create (amf-provision)

Overview This command sets up an empty directory on the backup media for use with a provisioned node. This directory can have configuration and release files copied to it from existing devices. Alternatively, the configuration files can be created by the user.

An alternative way to create a new provisioned node is with the command clone (amf-provision).

This command can only run on AMF master nodes.

Syntax

```
create
```

Mode AMF Provisioning

Usage notes This command is only available on master nodes in the AMF network.

A date and time is assigned to the new provisioning directory reflecting when this command was executed. If there is a backup or provisioned node with the same name on another AMF master then the most recent one will be used.

Example To create a new provisioned node named “device2” use the command:

```
device1# atmf provision node device2
device1(atmf-provision)# create
```

Running this command will create the following directories:

- <*media*>:atmf/<*atmf_name*>/nodes/<*node*>
- <*media*>:atmf/<*atmf_name*>/nodes/<*node*>/flash

To confirm the new node’s settings, use the command:

```
device1# show atmf backup
```

The output for the **show atmf backup** command is shown in the following figure, and shows details for the new provisioned node ‘device2’.

Figure 21-6: Sample output from the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 01 Oct 2018 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7315.2MB)
Server Config .........
  Synchronization ..... Unsynchronized
    Last Run .......... -
   1 .................. Unconfigured
   2 .................. Unconfigured
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

-----------------------------------------------------------------
Node Name     Date         Time      In ATMF  On Media  Status
-----------------------------------------------------------------
device2       -            -         No       Yes       Prov
device1       30 Sep 2018  00:05:49  No       Yes       Good
```

For instructions on how to configure on a provisioned node, see the AMF Feature Overview and Configuration Guide.

Related commands

atmf provision (interface)

atmf provision node

clone (amf-provision)

copy (amf-provision)

configure boot config (amf-provision)

configure boot system (amf-provision)

delete (amf-provision)

identity (amf-provision)

license-cert (amf-provision)

locate (amf-provision)

show atmf provision nodes

Command changes

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

debug atmf

Overview This command enables the AMF debugging facilities, and displays information that is relevant (only) to the current node. The detail of the debugging displayed depends on the parameters specified.

If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

The **no** variant of this command disables either all AMF debugging information, or only the particular information as selected by the command's parameters.

Syntax

```
debug atmf
[link|crosslink|arealink|database|neighbor|error|all]
```

```
no debug atmf
[link|crosslink|arealink|database|neighbor|error|all]
```

Parameter	Description
`link`	Output displays debugging information relating to uplink or downlink information.
`crosslink`	Output displays all crosslink events.
`arealink`	Output displays all arealink events.
`database`	Output displays only notable database events.
`neighbor`	Output displays only notable AMF neighbor events.
`error`	Output displays AMF error events.
`all`	Output displays all AMF events.

Default All debugging facilities are disabled.

Mode User Exec and Global Configuration

Usage notes If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

NOTE: *An alias to the **no** variant of this command is undebug atmf on page 820.*

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 - undebug atmf - can be found elsewhere in this chapter.*

Mode User Exec and Global Configuration

Usage notes If no additional parameters are specified, then the command output will apply a default selection of parameters shown below:

Parameter	Description
`direction`	Sets debug to packet received, transmitted, or both
`rx`	packets received by this node
`tx`	Packets sent from this node
`1`	AMF Packet Control header Information, Packet Sequence Number. Enter 1 to select this level.
`2`	AMF Detailed Packet Information. Enter 2 to select this level.
`3`	AMF Packet HEX dump. Enter 3 to select this level.
`timeout`	Sets the execution timeout for packet logging

Parameter	Description
<seconds>	Seconds
num-pkts	Sets the number of packets to be dumped
<quantity>	The actual number of packets
filter	Sets debug to filter packets
node	Sets the filter on packets for a particular Node
<name>	The name of the remote node
interface	Sets the filter to dump packets from an interface (portx.x.x) on the local node
<ifname>	Interface port or virtual-link
pkt-type	Sets the filter on packets with a particular AMF packet type
1	Crosslink Hello BPDU packet with crosslink links information. Enter 1 to select this packet type.
2	Crosslink Hello BPDU packet with downlink domain information. Enter 2 to select this packet type.
3	Crosslink Hello BPDU packet with uplink information. Enter 3 to select this packet type.
4	Downlink and uplink hello BPDU packets. Enter 4 to select this packet type.
5	Non broadcast hello unicast packets. Enter 5 to select this packet type.
6	Stack hello unicast packets. Enter 6 to select this packet type.
7	Database description. Enter 7 to select this packet type.
8	DBE request. Enter 8 to select this packet type.
9	DBE update. Enter 9 to select this packet type.
10	DBE bitmap update. Enter 10 to select this packet type.
11	DBE acknowledgment. Enter 11 to select this packet type.
12	Area Hello Packets. Enter 12 to select this packet type.
13	Gateway Hello Packets. Enter 13 to select this packet type.

Examples To set a packet debug on node 1 with level 1 and no timeout, use the command:

```
node_1# debug atmf packet direction tx timeout 0
```

To set a packet debug with level 3 and filter packets received from AMF node 1:

```
node_1# debug atmf packet direction tx level 3 filter node_1
```

To enable send and receive 500 packets only on vlink1 for packet types 1, 7, and 11, use the command:

```
node_1# debug atmf packet num-pkts 500 filter interface vlink1
pkt-type 1 7 11
```

delete (amf-provision)

Overview This command deletes files that have been created for loading onto a provisioned node. It can only be run on master nodes.

Syntax

```
delete
```

Mode AMF Provisioning

Usage notes This command is only available on master nodes in the AMF network. The command will only work if the provisioned node specified in the command has already been set up (although the device itself is still yet to be installed). Otherwise, an error message is shown when the command is run.

You may want to use the **delete** command to delete a provisioned node that was created in error or that is no longer needed.

This command cannot be used to delete backups created by the AMF backup procedure. In this case, use the command atmf backup delete to delete the files.

NOTE: *This command allows provisioned entries to be deleted even if they have been referenced by the atmf provision (interface) command, so take care to only delete unwanted entries.*

Example To delete backup files for a provisioned node named device3 use the command:

```
device1# atmf provision node device3
device1(atmf-provision)# delete
```

To confirm that the backup files for provisioned node device3 have been deleted use the command:

```
device1# show atmf backup
```

The output should show that the provisioned node device3 no longer exists in the backup file, as shown in the figure below:

Figure 21-7: Sample output showing the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 01 Oct 2016 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7297.0MB)
Server Config .........
  Synchronization ..... Unsynchronized
    Last Run .......... -
   1 .................. Unconfigured
   2 .................. Unconfigured
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

-----------------------------------------------------------------
Node Name     Date          Time      In ATMF  On Media  Status
-----------------------------------------------------------------
device1       30 Sep 2016   00:05:49  No       Yes       Good
device2       30 Sep 2016   00:05:44  Yes      Yes       Good
```

Related commands

atmf provision (interface)

atmf provision node

clone (amf-provision)

configure boot config (amf-provision)

configure boot system (amf-provision)

create (amf-provision)

identity (amf-provision)

license-cert (amf-provision)

locate (amf-provision)

show atmf provision nodes

Command changes

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

discovery

Overview Use this command to specify how AMF learns about guest nodes.

AMF nodes gather information about guest nodes by using one of the internally defined discovery methods: dynamic, static, or agent.

Dynamic learning (the default method) means that AMF learns the guest's IP and MAC addresses from LLDP or DHCP snooping. Dynamic learning is only supported when using IPv4. For IPv6, use static learning.

Static learning uses the switchport atmf-guestlink command to specify the guest class name and IP address of the guest node attached to each individual switch port. AMF then learns the MAC addresses of each of the guests of that class from ARP or Neighbor discovery tables.

If you are using the static method, ensure that you have configured the appropriate class type for each of your statically discovered guest nodes.

Agent learning uses the AMF agent to retrieve the guest's IP and MAC address. It is only available on guest nodes that support ATMF agent, such as TQ5403 series access points. For step-by-step instructions on using agent discovery for auto-recovery of an TQ5403 series AP, see the AMF Feature Overview and Configuration Guide.

The **no** variant of this command returns the discovery method to **dynamic**.

Syntax

```
discovery [dynamic|static|agent]
no discovery
```

Parameter	Description
`dynamic`	Learned from DCHCP Snooping or LLDP.
`static`	Statically assigned.
`agent`	Learned from the AMF agent.

Default Dynamic

Mode AMF Guest Configuration

Usage notes This command is one of several modal commands that are configured and applied for a specific guest-class (mode). Its settings are automatically applied to a guest-node link by the switchport atmf-guestlink command.

NOTE: *AMF guest nodes are not supported on ports using the OpenFlow protocol.*

Example 1 To configure static discovery for the guest-class 'camera', use the following commands:

```
Node1# configure terminal
Node1(config)# atmf guest-class camera
Node1(config-atmf-guest)# discovery static
```

Example 2 To return the discovery method for the guest class TQ6602 to its default of **dynamic**, use the following commands:

```
Node1# configure terminal
Node1(config)# atmf guest-class TQ6602
Node1(config-atmf-guest)# no discovery
```

Related commands

atmf guest-class

switchport atmf-guestlink

show atmf links guest

show atmf nodes

Command changes Version 5.5.3-0.1: **agent** parameter added

description (amf-container)

Overview Use this command to set the description on an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the AMF Feature Overview and Configuration Guide for more information on running multiple tenants on a single VAA host.

Use the **no** variant of this command to remove the description from an AMF container.

Syntax

```
description <description>
no description
```

Parameter	Description
<description>	Enter up to 128 characters of text describing the AMF container.

Mode AMF Container Configuration

Example To set the description for AMF container "vac-wlg-1" to "Wellington area", use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# description Wellington area
```

To remove the description for AMF container "vac-wlg-1", use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# no description
```

Related commands atmf container

show atmf container

Command changes Version 5.4.7-0.1: command added

erase factory-default

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

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

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

Syntax

```
erase factory-default
```

Mode Privileged Exec

Usage notes This command is an alias to the atmf cleanup command.

Example To erase data, use the command:

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

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

Related commands atmf cleanup

firmware-url

Overview Use this command to specify the location of an AP guest node's firmware file when preparing the AP for auto-recovery. AMF cannot back up AP firmware files (only configuration files), so you need to store the firmware file somewhere accessible and use this command to provide the AlliedWare Plus device with the file's location.

For step-by-step instructions for auto-recovery of an TQ5403 series AP, see the AMF Feature Overview and Configuration Guide.

Use the **no** variant of this command to remove the URL.

Syntax

```
firmware-url <name>
no firmware-url
```

Parameter	Description
<name>	The file's directory or filename. We recommend specifying a directory because that makes it easier to keep the firmware file up to date. The following protocols are supported: http, https, tftp, usb, and card. Do not change the firmware file's filename.

Default No URL is configured

Mode AMF Guest Configuration

Example To specify, on a device named node2, that the firmware file for a TQ5403 AP is stored in the top level of a USB stick, use the commands:

```
node2# configure terminal
node2(config)# atmf guest-class TQ5403
node2(config-guest)# firmware-url usb:
```

To specify, on a device named node2, that the firmware file for a TQ5403 AP is stored on a TFTP server with an address of 192.168.2.1, use the commands:

```
node2# configure terminal
node2(config)# atmf guest-class TQ5403
node2(config-guest)# firmware-url tftp://192.168.2.1/
```

Related commands

atmf guest-class

discovery

login-fallback enable

modeltype

show atmf guests

show atmf guests detail

switchport atmf-guestlink

Command changes Version 5.5.3-0.1: command added

http-enable

Overview This command is used to enable GUI access to a guest node. When **http-enable** is configured, the port number is set to its default of 80. If the guest node is using a different port for HTTP, you can configure this using the **port** parameter.

This command is used to inform the GUI that this device has an HTTP interface at the specified port number so that a suitable URL can be provided to the user.

Use the **no** variant of this command to disable HTTP.

Syntax

```
http-enable [port <port-number>]
no http-enable
```

Parameter	Description
`port`	TCP port number.
<port-number>	The port number to be configured.

Default Not set

Mode AMF Guest Configuration

Usage notes If **http-enable** is selected without a **port** parameter the port number will default to 80.

Example To enable HTTP access to a guest node on port 80 (the default), use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class Camera
node1(config-atmf-guest)# http-enable
```

To enable HTTP access to a guest node on port 400, use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class Camera
node1(config-atmf-guest)# http-enable port 400
```

To disable HTTP access to a guest node, use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class Camera
node1(config-atmf-guest)# no http-enable
```

Related commands

atmf guest-class

switchport atmf-guestlink

show atmf links guest

show atmf nodes

identity (amf-provision)

Overview Use this command to create an identity token for provisioning an isolated AMF node. An isolated node is an AMF member that is only connected to the rest of the AMF network via a virtual-link.

This command allows these nodes, which have no AMF neighbors, to be identified for provisioning purposes. They are identified using an identity token which is based on either the next-hop MAC address of the provisioned node, or the serial number of the device being provisioned. This identity token is stored on the AMF master.

Use the **no** variant of this command to remove the identity token for a node.

Syntax

```
identity mac-address <mac-address> prefix
<ip-address/prefix-length>
```

```
identity serial-number <serial-number> prefix
<ip-address/prefix-length>
```

```
no identity
```

Parameter	Description
`mac-address`	Specify the next-hop MAC address of the device being provisioned.
`<mac-address>`	MAC address of the port the provisioned node is connected to, in the format xxxx.xxxx.xxxx.
`serial-number`	Specify the serial number of the device to be provisioned.
`<serial-number>`	Serial number of the device that is being provisioned.
`prefix`	IPv4 address, and prefix length, of the virtual-link interface on the isolated node
`<ip-address/ prefix-length>`	IPv4 address, and prefix length, in A.B.C.D/M format.

Mode AMF Provisioning

Usage notes To provision an isolated node, first create a configuration for the node using the create (amf-provision) and/or the clone (amf-provision) commands.

Then create an identity token for the provisioned node by either specifying its next-hop MAC address or by specifying the serial number of the replacement device. The advantage of using the next-hop MAC address is that any device, regardless of its serial number, can be added to the network but using the serial number maybe preferred in situations where the next-hop MAC address is not easy to obtain.

The atmf recovery-server option must be enabled on the AMF master before attempting to provision the device. This option allows the AMF master to process recovery requests from isolated AMF nodes.

See the AMF Feature Overview and Configuration Guide for information on preparing your network for recovering or provisioning isolated nodes.

Example To create a identity token on your AMF master for a device named "my-x930" with serial number "A10064A172100008", use the command:

```
awplus# atmf provision node my-x930
awplus(atmf-provision)# identity serial-number
A10064A172100008 prefix 192.168.2.25/24
```

To create a identity token on your AMF master for a device named "my-x930" with next-hop MAC address "0000.cd28.0880", use the command:

```
awplus# atmf provision node my-x930
awplus(atmf-provision)# identity mac-address 0000.cd28.0880
prefix 192.168.2.25/24
```

To delete the identity token from your AMF master for a device named "my-x930", use the command:

```
awplus# atmf provision node my-x930
awplus(atmf-provision)# no identity
```

Related commands

atmf cleanup

atmf provision (interface)

atmf provision node

atmf recovery-server

atmf virtual-link

clone (amf-provision)

configure boot config (amf-provision)

configure boot system (amf-provision)

create (amf-provision)

delete (amf-provision)

license-cert (amf-provision)

locate (amf-provision)

show atmf provision nodes

Command changes

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

Version 5.4.7-2.1: command added

license-cert (amf-provision)

Overview

This command is used to set up the license certificate for a provisioned node.

The certificate file usually has all the license details for the network, and can be stored anywhere in the network. This command makes a hidden copy of the certificate file and stores it in the space set up for the provisioned node on AMF backup media.

For node provisioning, the new device has not yet been part of the AMF network, so the user is unlikely to know its product ID or its MAC address. When such a device joins the network, assuming that this command has been applied successfully, the copy of the certificate file will be applied automatically to the provisioned node.

Once the new device has been resurrected on the network and the certificate file has been downloaded to the provisioned node, the hidden copy of the certificate file is deleted from AMF backup media.

Use the **no** variant of this command to set it back to the default.

This command can only be run on AMF master nodes.

Syntax

```
license-cert <file-path|URL>
no license-cert
```

Parameter	Description
<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

AMF Provisioning

Usage notes

This command is only available on master nodes in the AMF network. It will only operate if the provisioned node specified in the command has already been set up, and if the license certification is present in the backup file. Otherwise, an error message is shown when the command is run.

Example 1

To apply the license certificate 'cert1.txt' stored on a TFTP server for AMF provisioned node "device2", use the command:

```
device1# atmf provision node device2
device1(atmf-provision)# license-cert
tftp://192.168.1.1/cert1.txt
```

Example 2

To apply the license certificate 'cert2.txt' stored in the AMF master's flash directory for AMF provisioned node 'host2', use the command:

```
device1# atmf provision node host2
device1(atmf-provision)# license-cert /cert2.txt
```

To confirm that the license certificate has been applied to the provisioned node, use the command show atmf provision nodes. The output from this command is shown below, and displays license certification details in the last line.

Figure 21-8: Sample output from the **show atmf provision nodes** command

```
device1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media .............: SD (Total 3827.0MB, Free 3481.1MB)

Node Name                 : device2
Date & Time               : 06-Oct-2016 & 23:25:44
Provision Path            : card:/atmf/nodes

Boot configuration :
Current boot image        : x510-5.4.6-1.4.rel (file exists)
Backup  boot image        : x510-5.4.6-1.3.rel (file exists)
Default boot config       : flash:/default.cfg (file exists)
Current boot config       : flash:/abc.cfg (file exists)
Backup  boot config       : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file           : ./.configs/.sw_v2.lic
                          : ./.configs/.swfeature.lic
Certificate file          : card:/atmf/lok/nodes/awplus1/flash/.atmf-lic-cert
```

Related commands

atmf provision (interface)

atmf provision node

clone (amf-provision)

configure boot config (amf-provision)

configure boot system (amf-provision)

create (amf-provision)

delete (amf-provision)

identity (amf-provision)

locate (amf-provision)

show atmf provision nodes

Command changes

Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

locate (amf-provision)

Overview This command changes the present working directory to the directory of a provisioned node. This makes it easier to edit files and create a unique provisioned node in the backup.

This command can only be run on AMF master nodes.

NOTE: *We advise that after running this command, you return to a known working directory, typically flash.*

Syntax

```
locate
```

Mode AMF Provisioning

Example To change the working directory that happens to be on device1 to the directory of provisioned node device2, use the following command:

```
device1# atmf provision node device2
device1[atmf-provision]# locate
```

The directory of the node device2 should now be the working directory. You can use the command pwd to check this, as shown in the following figure.

Figure 21-9: Sample output from the **pwd** command

```
device2#pwd
card:/atmf/building_2/nodes/device2/flash
```

The output above shows that the working directory is now the flash of device2.

Related commands

atmf provision (interface)

atmf provision node

clone (amf-provision)

configure boot config (amf-provision)

configure boot system (amf-provision)

copy (amf-provision)

create (amf-provision)

delete (amf-provision)

identity (amf-provision)

license-cert (amf-provision)

locate (amf-provision)

pwd

show atmf provision nodes

Command changes Version 5.4.9-0.1: syntax change due to new AMF provisioning mode

log event-host

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

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

Syntax

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

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

Default Log events are disabled by default.

Mode Global Configuration

Usage notes Event hosts are set so syslog sends the messages out as they come.

Note that there is a difference between log event and log host messages:

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

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

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

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

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

Related commands atmf topology-gui enable

login-fallback enable

Overview Use this command to enable login fallback on TQ model AMF guest nodes.This allows AMF to try the factory default username and password if the guest node's saved username and password fail.

Use the **no** variant of this command to disable login fallback.

Syntax

```
login-fallback enable
no login-fallback enable
```

Default Disabled

Mode AMF Guest Configuration

Usage notes This feature is only supported on TQ model guest nodes.

Login fallback means: if a guest node's saved username and password fail, AMF will try to connect to the node using the factory default username and password (manager/friend). When a new TQ replaces an existing TQ, this allows the new TQ to be discovered and managed as an AMF guest node. AMF can then start the AMF guest node recovery procedure.

Example To use the login fallback feature, first create an AMF guest class for TQ model APs. Then enable the login fall back feature.

For example, to enable login fallback on the guest-class AT-TQ5k, use the commands:

```
node1#configuration terminal
node1(config)#atmf guest-class AT-TQ5k
node1(config-atmf-guest)#login-fallback enable
node1(config-atmf-guest)#end
node1#
```

Related commands

atmf guest-class

modeltype

switchport atmf-guestlink

show atmf links guest

Command changes Version 5.5.0-1.1: command added

modeltype

Overview This command sets the expected model type of the guest node. The model type will default to **other** if nothing is set.

Use the **no** variant of this command to reset the model type to **other**.

Syntax

```
modeltype {alliedware|aw+|onvif|tq|other}
no modeltype
```

Parameter	Description
alliedware	A legacy Allied Telesis operating system.
aw+	The Allied Telesis AlliedWare Plus operating system.
onvif	ONVIF (Open Network Video Interface Forum) Profile Q devices
tq	An Allied Telesis TQ Series wireless access point.
other	Used where the model type is outside the above definitions.

Default Default to **other**

Mode AMF Guest Configuration

Examples To assign the model type **tq** to the guest-class called 'tq_device', use the commands:

```
node1# configure terminal
node1(config)# atmf guest-class tq_device
node1(config-atmf-guest)# modeltype tq
```

To remove the model type **tq** from the guest-class called 'tq_device', and reset it to the default of **other**, use the commands:

```
node1# configure terminal
node1(config)# atmf guest-class tq_device
node1(config-atmf-guest)# no modeltype
```

Related commands

atmf guest-class

switchport atmf-guestlink

show atmf links guest

Command changes Version 5.4.9-2.1: **onvif** parameter added

service atmf-application-proxy

Overview Use this command to enable the AMF Application Proxy service. This service distributes messages across all AMF nodes.

Currently this is used for threat protection. When an AMF Security (AMF-Sec) Controller detects a threat, it issues a request to block the address the threat originated from. The AMF Application Proxy service distributes this message to all AMF nodes. An AMF master accepts this block request and instructs the subordinate AMF node to block the relevant device.

Use the **no** variant of this command to disable the AMF Application Proxy service.

Syntax

```
service atmf-application-proxy
no service atmf-application-proxy
```

Default The AMF Application Proxy service is disabled by default.

Mode Global Configuration

Usage notes The AMF master maintains a list of all threats and will send this list to any AMF node, or VCS member, when it boots and joins the AMF network.

In order for this to work the follow must be configured:

- the AMF Application Proxy service on all AMF nodes that need to receive the messages.
- the Hypertext Transfer Protocol (HTTP) service on all nodes that are running the AMF Application Proxy service (see service http).

Example To enable the AMF Application Proxy service, use the commands

```
awplus# configure terminal
awplus(config)# service atmf-application-proxy
```

To disable the AMF Application Proxy service, use the commands

```
awplus# configure terminal
awplus(config)# no service atmf-application-proxy
```

Related commands

application-proxy threat-protection

application-proxy whitelist server

clear application-proxy threat-protection

show application-proxy threat-protection

Command changes Version 5.4.7-2.2: command added

show application-proxy threat-protection

Overview Use this command to list all the IP addresses blocked by the AMF Application Proxy service. It also shows the global threat-detection configuration.

Syntax
```
show application-proxy threat-protection [all]
```

Parameter	Description
`all`	Include information for non-local blocks.

Mode Privileged Exec

Example To list the addresses blocked by the AMF Application Proxy service, use the command:

```
awplus# show application-proxy threat-protection
```

Output Figure 21-10: Example output from **show application-proxy threat-protection**

```
awplus#show application-proxy threat-protection
Quarantine Vlan           : vlan200
Global IP-Filter          : Enabled
IP-Filter Limit Exceeded  : 0
Redirect-URL              : http://my.dom/help.html

Client IP        Interface    MAC Address     VLAN      Action
-----------------------------------------------------------------
10.34.199.110    -            -               -      link-down
10.34.199.116    port1.0.3    001a.eb93.ec5d  1           drop
10.1.179.1       *            *               *      ip-filter
...
```

Table 21-1: Parameters in the output from **show application-proxy threat-protection**

Parameter	Description
`Quarantine Vlan`	The name of the quarantine VLAN.
`Global IP-Filter`	The status of global IP filtering.
`IP-Filter Limit Exceeded`	The number of times an ACL failed to be installed due to insufficient space.
`Redirect-URL`	The URL a blocked user is redirected to.

Related commands
application-proxy quarantine-vlan

application-proxy threat-protection

clear application-proxy threat-protection

service atmf-application-proxy

Command changes

Version 5.4.7-2.2: command added

show application-proxy whitelist advertised-address

Overview Use this command to show the Layer 3 interface and its IPv4 address that is advertised as the application-proxy whitelist address.

Syntax
```
show application-proxy whitelist advertised-address
```

Mode Privileged Exec

Example To display the interface and IPv4 address advertised as the application-proxy whitelist address, use the command:

```
awplus# show application-proxy whitelist advertised-address
```

Output Figure 21-11: Example output from **show application-proxy whitelist advertised-address**

```
awplus#show application-proxy whitelist advertised-address
ATMF Application Proxy Whitelist advertised-address:
  Interface  : vlan1001
  IP address : 10.34.16.5
```

Related commands
application-proxy whitelist advertised-address

application-proxy whitelist server

Command changes Version 5.4.9-1.1: command added

show application-proxy whitelist interface

Overview Use this command to display the status of port authentication on the specified interface.

Syntax

```
show application-proxy whitelist interface [<interface-list>]
```

Parameter	Description
<interface-list>	The interfaces or ports to display information about. An interface-list can be: • a switchport (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 (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list. The specified interface must exist.

Mode Privileged Exec

Example To display the port authentication information for all interfaces, use the command:

```
awplus# show application-proxy whitelist interface
```

To display the port authentication information for port1.0.4, use the command

```
awplus# show application-proxy whitelist interface port1.0.4
```

Output Figure 21-12: Example output from **show application-proxy whitelist interface**

```
awplus#sh application-proxy whitelist interface
Authentication Info for interface port1.0.1
  portEnabled: false - portControl: Auto
  portStatus: Unknown
  reAuthenticate: disabled
  reAuthPeriod: 3600
  PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
  PAE: connectTimeout: 30
  BE: suppTimeout: 30 - serverTimeout: 30
  CD: adminControlledDirections: in
  KT: keyTxEnabled: false
  critical: disabled
  guestVlan: disabled
  guestVlanForwarding:
    none
  authFailVlan: disabled
  dynamicVlanCreation: disabled
  multiVlanSession: disabled
  hostMode: single-host
  dot1x: disabled
  authMac: enabled
    method: PAP
    scheme: mac
    reauthRelearning: disabled
  authWeb: disabled
  twoStepAuthentication:
    configured: disabled
    actual: disabled
  supplicantMac: none
  supplicantIpv4: none
Authentication Info for interface port1.0.2
...
```

Related commands

application-proxy whitelist enable

application-proxy whitelist server

show application-proxy whitelist server

show application-proxy whitelist supplicant

Command changes Version 5.4.9-0.1: command added

show application-proxy whitelist server

Overview Use this command to display the external RADIUS server details for the application-proxy whitelist feature.

Syntax

```
show application-proxy whitelist server
```

Mode Privileged Exec

Example To display the external RADIUS server details for the application-proxy whitelist feature, use the command:

```
awplus# show application-proxy whitelist server
```

Output Figure 21-13: Example output from **show application-proxy whitelist server**

```
awplus#show application-proxy whitelist server

Application Proxy Whitelist Details:

External Server Details:
 IP: 192.168.1.10
 Port: 2083
  Protection: TLS
  Trustpoint: None (Authentication disabled)

Proxy Details:
 IP: 172.31.0.5
 Status: Alive
```

Related commands

application-proxy whitelist enable

application-proxy whitelist server

show application-proxy whitelist interface

show application-proxy whitelist supplicant

Command changes Version 5.4.9-0.1: command added

show application-proxy whitelist supplicant

Overview Use this command to display the current configuration and status for each supplicant attached to an application-proxy whitelist port.

Syntax

```
show application-proxy whitelist supplicant [interface
<interface-list>|<mac-addr>|brief]
```

Parameter	Description
`interface <interface-list>`	The interfaces or ports to display information about. An interface-list can be: • a switchport (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 (e.g. port1.0.1,port1.0.3-1.0.4). Do not mix port types in the same list. The specified interface must exist.
`<mac-addr>`	MAC (hardware) address of the supplicant.Entry format is HHHH.HHHH.HHHH (hexadecimal)
`brief`	Brief summary of the supplicant state.

Mode Privileged Exec

Example To display the supplicant information for all ports, use the command:

```
awplus# show application-proxy whitelist supplicant
```

To display the supplicant information for port1.0.4, use the command:

```
awplus# show application-proxy whitelist supplicant interface
port1.0.4
```

Output Figure 21-14: Example output from **show application-proxy whitelist supplicant**

```
awplus#show application-proxy whitelist supplicant
Interface port1.0.4
  authenticationMethod: dot1x/mac/web
  Two-Step Authentication
    firstMethod: mac
    secondMethod: dot1x/web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0

  Supplicant name: test
  Supplicant address: 001c.233e.e15a
    authenticationMethod: WEB-based Authentication
    Two-Step Authentication:
      firstAuthentication: Pass - Method: mac
      secondAuthentication: Pass - Method: web
    portStatus: Authorized - currentId: 1
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 0
    CD: adminControlledDirections: in operControlledDirections: in
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    RADIUS server group (auth): radius
    RADIUS server (auth): 192.168.1.40
...
```

Related commands

application-proxy whitelist enable

application-proxy whitelist server

show application-proxy whitelist interface

show application-proxy whitelist server

Command changes Version 5.4.9-0.1: command added

show atmf

Overview Displays information about the current AMF node.

Syntax

```
show atmf [summary|tech|nodes|session]
```

Parameter	Description
summary	Displays summary information about the current AMF node.
tech	Displays global AMF information.
nodes	Displays a list of AMF nodes together with brief details.
session	Displays information on an AMF session.

Default Only summary information is displayed.

Mode User Exec and Privileged Exec

Usage notes AMF uses internal VLANs to communicate between nodes about the state of the AMF network. Two VLANs have been selected specifically for this purpose. Once these have been assigned, they are reserved for AMF and cannot be used for other purposes

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Example 1 To show summary information on AMF node_1 use the following command:

```
node_1# show atmf summary
```

Table 22: Output from the **show atmf summary** command

```
node_1#show atmf summary
ATMF Summary Information:

ATMF Status            : Enabled
Network Name           : Test_network
Node Name              : node_1
Role                   : Master
Restricted login       : Disabled
Current ATMF Nodes     : 3
```

Example 2 To show information specific to AMF nodes use the following command:

```
node_1# show atmf nodes
```

Example 3 The **show amf session** command displays all CLI (Command Line Interface) sessions for users that are currently logged in and running a CLI session.

To display AMF active sessions, use the following command:

```
node_1# show atmf session
```

For example, in the output below, node_1 and node_5 have active users logged in.

Table 23: Output from the **show atmf session** command

```
node_1#show atmf session

CLI Session Neighbors

Session ID                          : 73518
Node Name                           : node_1
PID                                 : 7982
Link type                           : Broadcast-cli
MAC Address                         : 0000.0000.0000
Options                             : 0
Our bits                            : 0
Link State                          : Full
Domain Controller                   : 0
Backup Domain Controller            : 0
Database Description Sequence Number : 00000000
First Adjacency                     : 1
Number Events                       : 0
DBE Retransmit Queue Length         : 0
DBE Request List Length             : 0
Session ID                          : 410804
Node Name                           : node_5
PID                                 : 17588
Link type                           : Broadcast-cli
MAC Address                         : 001a.eb56.9020
Options                             : 0
Our bits                            : 0
Link State                          : Full
Domain Controller                   : 0
Backup Domain Controller            : 0
Database Description Sequence Number : 00000000
First Adjacency                     : 1
Number Events                       : 0
DBE Retransmit Queue Length         : 0
DBE Request List Length             : 0
```

Example 4 The AMF tech command collects all the AMF commands, and displays them. You can use this command when you want to see an overview of the AMF network.

To display AMF technical information, use the following command:

```
node_1# show atmf tech
```

Table 24: 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 25: 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 25: 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). • VLAN ID - In this example VLAN 4092 is configured as the Management VLAN. • Management Subnet - Network prefix for the subnet. • Management IP Address - The IP address allocated for this traffic. • Management Mask - The subnet mask used to create a subnet for this traffic (255.255.128.0).
Domain VLAN	The VLAN assigned for traffic between Nodes of same domain (crosslink). • VLAN ID - In this example VLAN 4091 is configured as the domain VLAN. • Domain Subnet. The subnet address used for this traffic. • Domain IP Address. The IP address allocated for this traffic. • Domain Mask. The subnet mask used to create a subnet for this traffic (255.255.128.0).
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 26: Example output from the **show atmf area** command on a Controller.

```
controller-1#show atmf area

  ATMF Area Information:

  * = Local area

  Area               Area   Local         Remote        Remote         Node
  Name               ID     Gateway       Gateway       Master         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 27: Example output from the **show atmf area** command on a remote master.

```
Canterbury#show atmf area

  ATMF Area Information:

  * = Local area

  Area               Area   Local          Remote         Remote          Node
  Name               ID     Gateway        Gateway        Master          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 28: 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: • Reachable, if the link has been established. • 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 switchport atmf-arealink command. • 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. • Auth Start, which may indicate that the area names match on the controller and remote master, but the IDs do not match. • 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.? • Auth OK, which indicates that area authentication was successful and you can now use the atmf select-area command.
Remote Master	Whether the remote master node is reachable or not. This is N/A for the area of the controller or remote master on which the command is being run, because the master node on that device is local.
Node Count	The number of nodes in the area.
Area Count	The number of areas controlled by the controller.
Area Node Count	The total number of nodes in the area.

Example 2 To show detailed information about the areas, use the command:

```
controller-1# show atmf area detail
```

The following figure shows example output from running this command.

Table 29: Output from the **show atmf area detail** command

```
controller-1#show atmf area detail

 ATMF Area Detail Information:

 Controller distance       : 0

 Controller Id             : 21
 Backup Available          : FALSE

 Area Id                   : 2
 Gateway Node Name         : controller-1
 Gateway Node Id           : 342
 Gateway Ifindex           : 6013
 Masters Count             : 1
 Master Node Name          : well-master (329)
 Node Count                : 2

 Area Id                   : 3
 Gateway Node Name         : controller-1
 Gateway Node Id           : 342
 Gateway Ifindex           : 4511
 Masters Count             : 2
 Master Node Name          : cant1-master (15)
 Master Node Name          : cant2-master (454)
 Node Count                : 2
```

Related commands

show atmf area summary

show atmf area nodes

show atmf area nodes-detail

show atmf area guests

Overview This command will display details of all guests that the controller is aware of.

Syntax

```
show atmf area guests [<area-name> [<node-name>]]
```

Parameter	Description
<area-name>	The area name for guest information
<node-name>	The name of the node that connects to the guests.

Default n/a

Mode User Exec/Privileged Exec

Example 1 To display atmf area guest nodes on a controller, use the command,

```
GuestNode[1]#show atmf area guests
```

Output Figure 21-15: Example output from the **show atmf area guests** command

```
main-building Area Guest Node Information:
Device          MAC                                          IP/IPv6
Type            Address         Parent          Port         Address
-------------------------------------------------------------------------------
-               0008.5d10.7635  x230            1.0.3        192.168.5.4
AT-TQ4600       eccd.6df2.da60  wireless-node1  1.0.4        192.168.5.3
-               0800.239e.f1fe  x230            1.0.4        192.168.4.8
AT-TQ4600       001a.eb3b.dc80  wireless-node2  1.0.7        192.168.4.12

main-building guest node count 4

GuestNode[1]#
```

Table 30: Parameters in the output from **show atmf area guests** command

Parameter	Description
Device Type	The device type as read from the guest node.
MAC Address	The MAC address of the guest-node
Parent	The device that directly connects to the guest-node
Port	The port number on the parent node that connects to the guest node.
IP/IPv6	The IP or IPv6 address of the guest node.

Related commands

show atmf area

show atmf area nodes

show atmf backup guest

show atmf area guests-detail

show atmf area guests-detail

Overview This command displays the local and remote guest information from an AMF controller.

Syntax

```
show atmf area guests-detail [<area-name> [<node-name>]]
```

Parameter	Description
<area-name>	The name assigned to the AMF area. An area is an AMF network that is under the control of an AMF Controller.
<node-name>	The name assigned to the network node.

Default n/a.

Mode Privileged Exec

Example To display detailed information for all guest nodes attached to "node1", which is located within the area named "northern", use the following command:

```
AMF_controller#show atmf area guests-detail northern node1
```

Output Figure 21-16: Example output from the **show atmf guest detail** command.

```
#show atmf guest detail

Node Name                       : Node1
Port Name                       : port1.0.5
Ifindex                         : 5005
Guest Description               : tq4600
Device Type                     : AT-TQ4600
Configuration Mismatch          : No
Backup Supported                : Yes
MAC Address                     : eccd.6df2.da60
IP Address                      : 192.168.4.50
IPv6 Address                    : Not Set
HTTP Port                       : 80
Firmware Version                :
Node Name                       : poe
Port Name                       : port1.0.6
Ifindex                         : 5006
Guest Description               : tq3600
Device Type                     : AT-TQ2450
Configuration Mismatch          : No
Backup Supported                : Yes
MAC Address                     : 001a.eb3b.cb80
IP Address                      : 192.168.4.9
IPv6 Address                    : Not Set
HTTP Port                       : 80
Firmware Version                :
```

Table 31: Parameters shown in the output of the **show atmf guest detail** command

Parameter	Description
`Node Name`	The name of the guest's parent node.
`Port Name`	The port on the parent node that connects to the guest.
`IFindex`	An internal index number that maps to the port number on the parent node.
`Guest Description`	A brief description of the guest node as manually entered into the description (interface) command for the guest node port on the parent node.
`Device Type`	The device type as supplied by the guest node itself.
`Backup Supported`	Indicates whether AMF supports backup of this guest node.
`MAC Address`	The MAC address of the guest node.
`IP Address`	The IP address of the guest node.
`IPv6 Address`	The IPv6 address of the guest node.
`HTTP Port`	The HTTP port enables you to specify a port when enabling http to allow a URL for the http user interface of a Guest Node. This is determined by the http-enable command.
`Firmware Version`	The firmware version that the guest node is currently running.

Related commands

show atmf area nodes-detail

show atmf area guests

show atmf area nodes

Overview Use this command to display summarized information about an AMF controller's remote nodes.

Note that this command can only be run from a controller node.

Syntax `show atmf area nodes <area-name> [<node-name>]`

Parameter	Description
<area-name>	Displays information about nodes in the specified area.
<node-name>	Displays information about the specified node.

Mode Privileged Exec

Usage notes If you do not limit the output to a single area or node, this command lists all remote nodes that the controller is aware of. This can be a very large number of nodes.

Example To show summarized information for all the nodes in area 'Wellington', use the command:

```
controller-1# show atmf area nodes Wellington
```

The following figure shows partial example output from running this command.

Table 32: Output from the **show atmf area nodes Wellington** command

```
controller-1#show atmf area nodes Wellington

 Wellington Area Node Information:
 Node           Device              ATMF           Parent                      Node
 Name           Type                Master  SC     Domain                      Depth
 ---------------------------------------------------------------------------------
 well-gate      x230-18GP           N       N      well-master                 1
 well-master    AT-x930-28GPX       Y       N      none                        0

Wellington node count 2
```

Table 33: Parameter definitions from the **show atmf area nodes** command

Parameter	Definition
Node Name	The name assigned to a particular node.
Device Type	The Product series name.
ATMF Master	Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not).

Table 33: Parameter definitions from the **show atmf area nodes** command

Parameter	Definition
SC	The device configuration, one of C - Chassis (SBx8100 series), S - Stackable (VCS) or N - Standalone.
Parent Domain	The node to which the current node has an active uplink.
Node Depth	The number of nodes in the path from this node to the master node.

Related commands

show atmf area

show atmf area nodes-detail

show atmf area nodes-detail

Overview Use this command to display detailed information about an AMF controller's remote nodes.

Note that this command can only be run from a controller node.

Syntax

```
show atmf area nodes-detail <area-name> [<node-name>]
```

Parameter	Description
<area-name>	Displays detailed information about nodes in the specified area.
<node-name>	Displays detailed information about the specified node.

Mode Privileged Exec

Usage notes If you do not limit the output to a single area or node, this command displays information about all remote nodes that the controller is aware of. This can be a very large number of nodes.

Example To show information for all the nodes in area 'Wellington', use the command:

```
controller-1# show atmf area nodes-detail Wellington
```

The following figure shows partial example output from running this command.

Table 34: Output from the **show atmf area nodes-detail Wellington** command

```
controller-1#show atmf area nodes-detail Wellington

Wellington Area Node Information:
  Node name  well-gate
  Parent node name    : well-master
  Domain id           : well-gate's domain
  Board type          : 368
  Distance to core    : 1
  Flags               : 50
  Extra flags         : 0x00000006
  MAC Address         : 001a.eb56.9020

Node name well-master
  Parent node name    : none
  Domain id           : well-master's domain
  Board type          : 333
  Distance to core    : 0
  Flags               : 51
  Extra flags         : 0x0000000c
  MAC Address         : eccd.6d3f.fef7

...
```

Table 35: Parameter definitions from the **show atmf area nodes-detail** command

Parameter	Definition
`Node name`	The name assigned to a particular node.
`Parent node name`	The node to which the current node has an active uplink.
`Domain id`	The name of the domain the node belongs to.
`Board type`	The Allied Telesis code number for the device.
`Distance to core`	The number of nodes in the path from the current node to the master node in its area.
`Flags`	Internal AMF information
`Extra flags`	Internal AMF information
`MAC Address`	The MAC address of the current node

Related commands show atmf area

show atmf area nodes

show atmf area summary

Overview Use this command to display a summary of IPv6 addresses used by AMF, for one or all of the areas controlled by an AMF controller.

Syntax

```
show atmf area summary [<area-name>]
```

Parameter	Description
<area-name>	Displays information for the specified area only.

Mode Privileged Exec

Example 1 To show a summary of IPv6 addresses used by AMF, for all of the areas controlled by controller-1, use the command:

```
controller-1# show atmf area summary
```

The following figure shows example output from running this command.

Table 36: Output from the **show atmf area summary** command

```
controller-1#show atmf area summary

 ATMF Area Summary Information:

Management Information
 Local IPv6 Address              : fd00:4154:4d46:1::15

Area Information
 Area Name                       : NZ (Local)
 Area ID                         : 1
 Area Master IPv6 Address        : -

 Area Name                       : Wellington
 Area ID                         : 2
 Area Master IPv6 Address        : fd00:4154:4d46:2::149

 Area Name                       : Canterbury
 Area ID                         : 3
 Area Master IPv6 Address        : fd00:4154:4d46:3::f

 Area Name                       : Auckland
 Area ID                         : 100
 Area Master IPv6 Address        : fd00:4154:4d46:64::17
 Interface                       : vlink2000
```

Related commands

show atmf area

show atmf area nodes

show atmf area nodes-detail

show atmf authorization

Overview Use this command on an AMF master to display the authorization status of other AMF members and masters on the network.

On an AMF controller this command will show the authorization status of remote area AMF masters.

Syntax

```
show atmf authorization {current|pending|provisional}
```

Parameter	Description
`current`	Show the status of all authorized nodes.
`pending`	Show the status of unauthorized nodes in the pending queue. These are nodes that enabled secure mode with atmf secure-mode but have not yet been authorized with atmf authorize.
`provisional`	Show the status of provisionally authorized nodes. These are nodes that have been provisioned with atmf authorize provision.

Mode Privileged Exec

Example To display all authorized AMF nodes on an AMF controller or AMF master, use the command:

```
awplus# show atmf authorization current
```

To display AMF nodes which are requesting authorization on an AMF controller or AMF master, use the command:

```
awplus# show atmf authorization pending
```

To display AMF nodes which have provisional authorization, use the command:

```
awplus# show atmf authorization provisional
```

Output Figure 21-17: Example output from **show atmf authorization current**

```
  NZ Authorized Nodes:
  Node Name             Signer                Expires
-----------------------------------------------------------------
  master_1              master_1              4 Mar 2017
  area_1_node_1         master_1              4 Mar 2017
  area_1_node_2         master_1              4 Mar 2017
```

Table 21-1: Parameters in the output from **show atmf authorization current**

Parameter	Description
Node Name	AMF node name of the authorized node.
Signer	Name of the AMF master that authorized the node.
Expires	Expiry date of the authorization. Authorization expiry time is set using atmf secure-mode certificate expiry.

Output Figure 21-18: Example output from **show atmf authorization pending**

```
  Pending Authorizations:

  NZ Requests:
  Node Name            Product          Parent Node      Interface
-------------------------------------------------------------------
  area_1_node_3        x230-18GP        master_1         port1.2.9
  area_1_node_4        x510-52GTX       master_1         sa1
```

Table 21-2: Parameters in the output from **show atmf authorization pending**

Parameter	Description
Node Name	Name of the node that is requesting authorization.
Product	Product name.
Parent Node	Authorization authority of the requesting node.
Interface	Interface that the authorization request came in on.

Output Figure 21-19: Example output from **show atmf authorization provisional**

```
 ATMF Provisional Authorization:

  Area - Node Name                  Start                  Timeout
  or MAC Address       Interface    Time                   Minutes
-------------------------------------------------------------------
  3333.4444.5555                    5 Sep 2016 02:35:54     3
  1111.2222.3333                    5 Sep 2016 02:35:24     60
  NZ - blue            port1.0.3    5 Sep 2016 02:35:06     60
```

Table 21-3: Parameters in the output from **show atmf authorization provisional**

Parameter	Description
`Area - Node Name or MAC Address`	MAC address or node name of the node that has been provisionally authorized.
`Interface`	Interface that the node has been provisioned on.
`Start Time`	Time the node was provisioned.
`Timeout Minutes`	Length of time from `Start Time` until the provisional authorization expires.

Related commands

atmf authorize

atmf authorize provision

atmf secure-mode

clear atmf secure-mode certificates

show atmf

show atmf secure-mode

show atmf secure-mode certificates

Command changes

Version 5.4.7-0.3: command added

show atmf backup

Overview This command displays information about AMF backup status for all the nodes in an AMF network. It can only be run on AMF master and controller nodes.

Syntax

```
show atmf backup
show atmf backup logs
show atmf backup server-status
show atmf backup synchronize [logs]
```

Parameter	Description
`logs`	Displays detailed log information.
`server-status`	Displays connectivity diagnostics information for each configured remote file server.
`synchronize`	Display the file server synchronization status
`logs`	For each remote file server, display the logs for the last synchronization

Mode Privileged Exec

Example 1 To display the AMF backup information, use the command:

```
node_1# show atmf backup
```

To display log messages to do with backups, use the command:

```
node_1# show atmf backup logs
```

Table 21-4: Output from **show atmf backup**

```
Node_1# show atmf backup
ScheduledBackup ......Enabled
  Schedule............1 per day starting at 03:00
  Next Backup Time....04 May 2019 03:00
Backup Bandwidth .....Unlimited
Backup Media..........SD (Total 1974.0 MB, Free197.6MB)
Current Action........Starting manual backup
Started...............04 May 2019 10:08
CurrentNode...........atmf_testbox1
Backup Redundancy ....Enabled
  Local media ........SD (Total 3788.0MB, Free 3679.5MB)
  State ..............Active

Node Name                Date         Time      In ATMF  On Media   Status
-------------------------------------------------------------------------------
atmf_testbox1            04 May 2019  09:58:59  Yes      Yes        In Progress
atmf_testbox2            04 May 2019  10:01:23  Yes      Yes        Good
```

Table 21-5: Output from **show atmf backup logs**

```
Node_1#show atmf backup logs

Backup Redundancy ..... Enabled
Local media ......... SD (Total 3788.0MB, Free 1792.8MB)
State ............... Inactive (Remote file server is not available)

Log File Location: card:/atmf/ATMF/logs/rsync_<node name>.log

Node
Name Log Details
-------------------------------------------------------------------------------
atmf_testbox
2019/05/04 18:16:51 [9045] receiving file list
2019/05/04 18:16:51 [9047] .d..t.... flash/
2019/05/04 18:16:52 [9047] >f+++++++ flash/a.rel
```

Example 2 To display the AMF backup synchronization status, use the command:

```
node_1# show atmf backup synchronize
```

To display log messages to do with synchronization of backups, use the command:

```
node_1# show atmf backup synchronize logs
```

Table 21-6: Output from **show atmf backup synchronize**

```
Node_1#show atmf backup synchronize

ATMF backup synchronization:

 * = Active file server

  Id  Date          Time       Status
-------------------------------------------------------------------
  1   04 May 2016   22:25:57   Synchronized
* 2   -             -          Active
```

Table 21-7: Output from **show atmf backup synchronize logs**

```
Node_1#show atmf backup synchronize logs

Id    Log Details
-------------------------------------------------------------------------------
1     2019/05/04 22:25:54 [8039] receiving file list
      2019/05/04 22:25:54 [8039] >f..t.... backup_Box1.info
      2019/05/04 22:25:54 [8039] sent 46 bytes received 39 bytes total size 40
```

Example 3 To display the AMF backup information with the optional parameter **server-status**, use the command:

```
Node_1# show atmf backup server-status
```

```
Node1#sh atmf backup server-status

Id   Last Check    State
-------------------------------------
1    186 s         File server ready
2    1 s           SSH no route to host
```

Table 22: Parameter definitions from the **show atmf backup** command

Parameter	Definition
Scheduled Backup	Indicates whether AMF backup scheduling is enabled or disabled.
Schedule	Displays the configured backup schedule.
Next Backup Time	Displays the date and time of the next scheduled.
Backup Media	The current backup medium in use. Utilized and available memory (MB) will be indicated if backup media memory is present.
Current Action	The task that the AMF backup mechanism is currently performing. This will be a combination of either (Idle, Starting, Doing, Stopping), or (manual, scheduled).
Started	The date and time that the currently executing task was initiated in the format DD MMM YYYY HH:MM
Current Node	The name of the node that is currently being backed up.
Backup Redundancy	Whether backup redundancy is enabled or disabled.
Local media	The local media to be used for backup redundancy; SD, USB, INTERNAL, or NONE, and total and free memory available on the media.
State	Whether SD or USB media is installed and available for backup redundancy. May be Active (if backup redundancy is functional—requires both the local redundant backup media and a remote server to be configured and available) or Inactive.
Node Name	The name of the node that is storing backup data - on its backup media.
Date	The data of the last backup in the format DD MMM YYYY.
Time	The time of the last backup in the format HH:MM:SS.
In ATMF	Whether the node shown is active in the AMF network, (Yes or No).
On Media	Whether the node shown has a backup on the backup media (Yes or No).

Table 22: Parameter definitions from the **show atmf backup** command (cont.)

Parameter	Definition
`Status`	The output can contain one of four values: • "-" meaning that the status file cannot be found or cannot be read. • "Errors" meaning that there are issues - note that the backup may still be deemed successful depending on the errors. • "Stopped" meaning that the backup attempt was manually aborted. • "Good" meaning that the backup was completed successfully. • "In Progress" meaning that the backup is currently running on that node.
`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: card:/amf/office/logs/rsync_amf_testbox1.log.
`Log Details`	The contents of the backup log file.
`server-status`	Displays connectivity diagnostics information for each configured remove file server.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Related commands

show atmf

atmf network-name

show atmf backup area

Overview Use this command to display backup status information for the master nodes in one or more areas.

Note that this command is only available on AMF controllers.

Syntax `show atmf backup area [<area-name> [<node-name>]] [logs]`

Parameter	Description
`logs`	Displays the logs for the last backup of each node.
`<area-name>`	Displays information about nodes in the specified area.
`<node-name>`	Displays information about the specified node.

Mode Privileged Exec

Example To show information about backups for an area, use the command:

```
controller-1# show atmf backup area
```

Table 23: Output from the **show atmf backup area** command

```
controller-1#show atmf backup area

Scheduled Backup ...... Enabled
  Schedule ............ 12 per day starting at 14:30
  Next Backup Time .... 15 Oct 2016 04:30
Backup Bandwidth ...... Unlimited
Backup Media .......... FILE SERVER 1 (Total 128886.5MB, Free 26234.2MB)
Server Config .........
 * 1 .................. Configured   (Mounted, Active)
    Host ............... 10.37.74.1
    Username ........... root
    Path ............... /tftpboot/backups_from_controller-1
    Port ............... -
   2 .................. Configured   (Unmounted)
    Host ............... 10.37.142.1
    Username ........... root
    Path ............... -
    Port ............... -
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

Backup Redundancy ..... Enabled
  Local media ......... USB (Total 7604.0MB, Free 7544.0MB)
  State ............... Active

Area Name          Node Name            Id   Date          Time       Status
-------------------------------------------------------------------------------
Wellington         camry                1    14 Oct 2016   02:30:22   Good
Canterbury         corona               1    14 Oct 2016   02:30:23   Good
Canterbury         Avensis              1    14 Oct 2016   02:30:22   Good
Auckland           RAV4                 1    14 Oct 2016   02:30:23   Good
Southland          MR2                  1    14 Oct 2016   02:30:24   Good
```

Related commands

atmf backup area-masters enable

show atmf area

show atmf area nodes-detail

switchport atmf-arealink

show atmf backup guest

Overview This command displays backup status information of guest nodes in an AMF network.This command can only be run on a device configured as an AMF Master and has an AMF guest license.

Syntax

```
show atmf backup guest [<node-name> [<guest-port>]] [logs]
```

Parameter	Description
<node-name>	The name of parent guest node
<guest-port>	The port number on the parent node

Mode User Exec/Privileged Exec

Example On the switch named x930-master, to display information about the AMF backup guest status, use the command:

```
x930-master# show atmf backup guest
```

Output Figure 21-20: Example output from **show atmf backup guest**

```
x930-master#sh atmf backup guest
Guest Backup .......... Enabled
Scheduled Backup ...... Disabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 20 Jan 2016 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... FILE SERVER 2 (Total 655027.5MB,
                        Free 140191.5MB)
Server Config
 1 ................... Configured (Mounted)
 Host ............... 11.0.24.1
 Username ........... bob
 Path ............... guest-project
 Port ............... -
* 2 ................... Configured (Mounted, Active)
 Host ............... 11.0.24.1
 Username ........... bob
 Path ............... guest-project-second
Port..................-
Current Action .......Idle
Started ............. -
Current Node ........ -
Backup Redundancy ....Enabled
Local media ......... USB (Total 7376.0MB, Free 7264.1MB)
State ............... Active
```

```
Parent Node Name      Port Name        Id     Date           Time          Status
-------------------------------------------------------------------------------
x230                  port1.0.4        2      19 Jan 2016    22:21:46      Good
                                       1      19 Jan 2016    22:21:46      Good
                                       USB    19 Jan 2016    22:21:46      Good
```

Table 21-1: Parameters in the output from **show atmf backup guest**

Parameter	Description
Guest Backup	The status of the guest node backup process
Scheduled Backup	The timing configured for guest backups.
Schedule	Displays the configured backup schedule.
Next Backup Time	The time the next backup process will be initiated.
Backup Bandwidth	The bandwidth limit applied to the backup data flow measured in kilo Bytes /second. Note that unlimited means there is no limit set specifically for the backup data flow.
Backup Media	Detail of the memory media used to store the backup files and the current memory capacity available.

Related commands

show atmf backup area

show atmf backup

show atmf links guest

show atmf nodes

show atmf backup guest

atmf backup guests delete

atmf backup guests enable

show atmf container

Overview Use this command to display information about the AMF containers created on a a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the AMF Feature Overview and_Configuration Guide for more information on running multiple tenants on a single VAA host.

Syntax

```
show atmf container [detail] [<container-name>]
```

Parameter	Description
`detail`	Show detailed information.
<container-name>	The name of the AMF container you wish to display information for.

Mode Privileged Exec

Output Figure 21-21: Example output from **show atmf container**

```
awplus#show atmf container

ATMF Container Information:

  Container       Area        Bridge   State      Memory    CPU%
-------------------------------------------------------------------
  vac-wlg-1       wlg         br1      running    70.3 MB   1.2
  vac-akl-1       akl         br2      stopped    0 bytes   0.0
  vac-nsn-1       nsn         br3      running    53.2 MB   0.7

Current ATMF Container count: 3
```

Figure 21-22: Example output from **show atmf container vac-wlg-1**

```
awplus#show atmf container vac-wlg-1

ATMF Container Information:

  Container       Area        Bridge   State      Memory    CPU%
-------------------------------------------------------------------
  vac-wlg-1       wlg         br1      running    70.3 MB   1.2

Current ATMF Container count: 1
```

Table 21-2: Parameters in the output from **show atmf container**

Parameter	Description
Container	Name of the AMF container.
Area	Name of the area the container is in.
Bridge	Name of the bridge connecting the container to the physical network.
State	Container state, running or stopped. This is set with the state command.
Memory	The amount of memory the container is using on the VAA host.
CPU%	The percentage of CPU time the container is using on the VAA, at the time the show command is run.

Figure 21-23: Example output from **show atmf container detail vac-wlg-1**

```
awplus#show atmf container detail vac-wlg-1

ATMF Container Information:

Name: vac-wlg-1
State: RUNNING
PID: 980
IP: 172.31.0.1
IP: 192.168.0.2
IP: fd00:4154:4d46:3c::1
CPU use: 3.95 seconds
Memory use: 67.07 MiB
Memory use: 0 bytes
Link: vethP31UFA
TX bytes: 166.01 KiB
RX bytes: 141.44 KiB
Total bytes: 307.45 KiB
Link: vethYCT7BB
TX bytes: 674.27 KiB
RX bytes: 698.27 KiB
Total bytes: 1.34 MiB
```

Table 21-3: Parameters in the output from **show atmf container detail**

Parameter	Description
Name	Name of the AMF container.
State	Container state, RUNNING or STOPPED. This is set with the state command.

Table 21-3: Parameters in the output from **show atmf container detail** (cont.)

Parameter	Description
PID	Internal container id.
IP	This lists the IP addresses used by the container. These include the eth1 IP address and the AMF management IP address.
CPU use	The CPU usage of the container since it was enabled.
Memory use	Container memory usage.
Link	Each container has two links: 1 An AMF area-link, this connects the container to the AMF controller and uses virtual interface eth0 on the AMF container. 2 A bridged L2 network link, this connects the container to the outside world and uses the virtual interface eth1 on the AMF container. See the AMF Feature Overview and Configuration_Guide for more information on these links.
TX/RX bytes	Bytes sent and received on a link.
Total bytes	Total bytes transferred on a link.

Related commands

area-link

atmf area

atmf area password

atmf container

atmf container login

bridge-group (amf-container)

description (amf-container)

state

Command changes

Version 5.4.7-0.1: command added

show atmf detail

Overview This command displays details about an AMF node. It can only be run on AMF master and controller nodes.

Syntax

```
show atmf detail
```

Parameter	Description
`detail`	Displays output in greater depth.

Mode Privileged Exec

Example 1 To display the AMF node1 information in detail, use the command:

```
controller-1# show atmf detail
```

A typical output screen from this command is shown below:

```
atmf-1#show atmf detail
ATMF Detail Information:

Network Name                        : Test_network
Network Mtu                         : 1300
Node Name                           : controller-1
Node Address                        : controller-1.atmf
Node ID                             : 342
Node Depth                          : 0
Domain State                        : BackupDomainController
Recovery State                      : None
Recovery Over ETH Ports             : Disabled
Log Verbose Setting                 : Verbose
Topology GUI                        : Disabled

Management VLAN
 VLAN ID                            : 4000
 Management Subnet                  : 172.31.0.0
 Management IP Address              : 172.31.1.86
 Management Mask                    : 255.255.128.0
 Management IPv6 Address            : fd00:4154:4d46:1::156
 Management IPv6 Prefix Length      : 64

Domain VLAN
 VLAN ID                            : 4091
 Domain Subnet                      : 172.31.128.0
 Domain IP Address                  : 172.31.129.86
 Domain Mask                        : 255.255.128.0
```

Table 22: Parameter definitions from the **show atmf detail** command

Parameter	Definition
`Network MTU`	The network MTU for the ATMF network.
`Network Name`	The AMF network that a particular node belongs to.
`Node Name`	The name assigned to a particular node.
`Node Address`	An address used to access a remotely located node. This is simply the Node Name plus the dotted suffix atmf (.atmf).
`Node ID`	A unique identifier assigned to a node on an AMF network.
`Node Depth`	The number of nodes in the path from this node to the level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.
`Domain State`	The state of a node in a Domain in an AMF network as Controller/Backup.
`Recovery State`	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.
`Recovery Over ETH Ports`	Allow AMF recovery over the Eth port on an AR-series device.
`Log Verbose Setting`	The state of the atmf log-verbose command.
`Topology GUI`	This feature allows your AMF network to interact with Vista Manager EX and must be enabled on your AMF master.
`Management VLAN`	The VLAN created for traffic between nodes of different domain (up/down links). • VLAN ID - in this example VLAN 4092 is configured as the Management VLAN. • Management Subnet - the network prefix for the subnet. • Management IP Address - the IP address allocated for this traffic. • Management Mask - the subnet mask used to create a subnet for this traffic (255.255.128.0).
`Domain VLAN`	The VLAN assigned for traffic between nodes of the same domain (crosslink). • VLAN ID - in this example VLAN 4091 is configured as the domain VLAN. • Domain Subnet - the subnet address used for this traffic. • Domain IP Address - the IP address allocated for this traffic. • Domain Mask - the subnet mask used to create a subnet for this traffic (255.255.128.0).
`Node Depth`	The number of nodes in the path from this node to the core domain.

show atmf group

Overview This command can be used to display the group membership within to a particular AMF node. It can also be used with the working-set command to display group membership within a working set.

Each node in the AMF is automatically added to the group that is appropriate to its hardware architecture, e.g. x510, x230. Nodes that are configured as masters are automatically assigned to the master group.

You can create arbitrary groups of AMF members based on your own selection criteria. You can then assign commands collectively to any of these groups.

Syntax

```
show atmf group [user-defined|automatic]
```

Parameter	Description
`user-defined`	User-defined-group information display.
`automatic`	Automatic group information display.

Default All groups are displayed

Mode Privileged Exec

Example 1 To display group membership of node2, use the following command:

```
node2# show atmf group
```

A typical output screen from this command is shown below:

```
ATMF group information

master, x510

node2#
```

This screen shows that node2 contains the groups **master** and **x510**. Note that although the node also contains the implicit groups, these do not appear in the show output.

Example 2 The following commands (entered on *node2*) will display all the automatic groups within the working set containing *node1* and all nodes that have been pre-defined to contain the *sysadmin* group:

First define the working-set:

```
node1# #atmf working-set node1 group sysadmin
```

A typical output screen from this command is shown below:

```
ATMF group information

master, poe, x8100


================================================
node1, node2, node3, node4, node5, node6:
================================================

ATMF group information

sysadmin, x8100

AMF_NETWORK[6]#
```

This confirms that the six nodes (*node1* to *node6*) are now members of the working-set and that these nodes reside within the *AMF-NETWORK*.

Note that to run this command, you must have previously entered the command atmf working-set on page 668. This can be seen from the network level prompt, which in this case is *AMF_NETWORK[6]#*.

Table 23: 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 24: Parameter definitions from the **show atmf group** command for a working set

Parameter	Definition
`ATMF group information`	Displays a list of nodes and the groups that they belong to, for example: • master - Shows a common group name for Nodes configured as AMF masters. • Hardware Arch - Shows a group for all Nodes sharing a common Hardware architecture, e.g. x8100, x230, for example. • User-defined - Arbitrary groups created by the user for AMF nodes.

show atmf group members

Overview This command will display all group memberships within an AMF working-set. Each node in the AMF working set is automatically added to automatic groups which are defined by hardware architecture, e.g. x510, x230. Nodes that are configured as masters are automatically assigned to the master group. Users can define arbitrary groupings of AMF members based on their own criteria, which can be used to select groups of nodes.

Syntax

```
show atmf group members [user-defined|automatic]
```

Parameter	Description
`user-defined`	User defined group membership display.
`automatic`	Automatic group membership display.

Mode Privileged Exec

Example To display group membership of all nodes in a working-set, use the command:

```
ATMF_NETWORK[9]# show atmf group members
```

Table 25: Sample output from the **show atmf group members** command

```
ATMF Group membership

Automatic        Total
Groups           Members   Members
-----------------------------------------------------------
master           1         Building_1
poe              1         HW_Team1
x510             3         SW_Team1 SW_Team2 SW_Team3
x930             1         HW_Team1
x8100            2         Building_1 Building_2

ATMF Group membership

User-defined     Total
Groups           Members   Members
-----------------------------------------------------------
marketing          1       Bld1_Floor_1
software           3       SW_Team1 SW_Team2 SW_Team3
```

Table 26: Parameter definitions from the **show atmf group members** command

Parameter	Definition
`Automatic Groups`	Lists the Automatic Groups and their nodal composition. The sample output shows AMF nodes based on the same Hardware type or belonging to the same Master group.
`User-defined Groups`	Shows the grouping of AMF nodes in user defined groups.
`Total Members`	Shows the total number of members in each group.
`Members`	Shows the list of AMF nodes in each group.

Related commands

show atmf group

show atmf

atmf group (membership)

show atmf guests

Overview This command is available on any AMF master or controller in the network. It displays a summary of the AMF guest nodes that exist in the AMF network, including device type, parent node, and IP address.

Syntax
```
show atmf guests
```

Mode User Exec/Privileged Exec

Usage notes Use this command to display all guest nodes in a network. If you want to see only the guests attached to a single node, use the show atmf links guest command, which shows information about the guest nodes and also about their link to their parent node.

Example To display the AMF guest output, use the command:

```
awplus# show atmf guests
```

Output Figure 21-24: Example output from the **show atmf guests** command

```
master#show atmf guests

  Guest Information:

  Device          Device          Parent      Guest     IP/IPv6
  Name            Type            Node        Port      Address
-------------------------------------------------------------------------
  node1-2.0.1     x600-24Ts       node1       2.0.1     192.168.2.10
  wireless-zone1  AT-TQ4600       node2       1.0.1     192.168.1.10
  wireless-zone2  AT-TQ4600       node2       1.0.2     192.168.1.12

  Current ATMF guest node count 3
```

Table 27: Parameters shown in the output of the **show atmf guests** command

Parameter	Description
Device Name	The name that is discovered from the device, or failing that, a name that is auto-assigned by AMF. The auto-assigned name consists of: <parent node name>-<attached port number> You can change this by configuring a description on the port.
Device Type	The product name of the guest node, which is discovered from the device. If no device type can be discovered, this shows the name of the AMF guest-class that has been assigned to the guest node by the atmf guest-class command.

Table 27: Parameters shown in the output of the **show atmf guests** command

Parameter	Description
`Parent Node`	The name of the AMF node that directly connects to the guest node.
`Guest Port`	The port on the parent node that directly connects to the guest node.
`IP/IPv6 Address`	The address discovered from the node, or statically configured on the parent node's attached port.

Related commands

atmf guest-class

switchport atmf-guestlink

show atmf backup guest

show atmf links guest

show atmf guests detail

Overview This command is available on any AMF master in the network. It displays details about the AMF guest nodes that exist in the AMF network, such as device type, IP address, MAC address etc.

Syntax

```
show atmf guests detail [<node-name>] [<guest-port>]
```

Parameter	Description
<node-name>	The name of the guest node's parent.
<guest-port>	The port name on the parent node.

Mode User Exec/Privileged Exec

Usage notes If you want to see only the guests attached to a single node, you can use either:

- this command and specify the node name, or
- show atmf links guest detail, which shows information about the guest nodes and also about their link to their parent node.

Note that the parameters that are displayed depend on the guest node's model.

Example To display the AMF guest output, use the command:

```
awplus# show atmf guests detail
```

Output Figure 21-25: Example output from **show atmf guests detail**

```
master#show atmf guests detail

ATMF Guest Node Information:

Node Name                       : master
Port Name                       : port1.0.9
Ifindex                         : 5009
Guest Description               : red-1.0.9
Device Type                     : x600-24Ts
Backup Supported                : No
MAC Address                     : 0000.cd38.0c4d
IP Address                      : 192.168.1.5
IPv6 Address                    : Not Set
HTTP Port                       : 0
Firmware Version                : 5.4.2-0.1
```

```
Node Name                       : node1
Port Name                       : port1.0.13
Ifindex                         : 5013
Guest Description               : node1-1.0.13
Device Type                     : AT-TQ4600
Backup Supported                : Yes
MAC Address                     : eccd.6df2.daa0
IP Address                      : 192.168.5.6
IPv6 Address                    : Not Set
HTTP Port                       : 80
Firmware Version                : 3.1.0 B01
```

Table 28: Parameters in the output from **show atmf guests detail**.

Parameter	Description
Node Name	The name of the parent node, which is the AMF node that directly connects to the guest node.
Port Name	The port on the parent node that connects to the guest.
IfIndex	An internal index number that maps to the port number on the parent node.
Guest Description	A description that is discovered from the device, or failing that, auto-assigned by AMF. The auto-assigned name consists of: <parent node name>-<attached port number>. You can change this by configuring a description on the port.
Device Type	The product name of the guest node, which is discovered from the device. If no device type can be discovered, this shows the name of the AMF guest-class that has been assigned to the guest node by the atmf guest-class command.
Username	The user name configured on the guest node.
Backup Supported	Whether the guest node supports AMF backup functionality.
MAC Address	The MAC address of the guest node.
IP Address	The IP address of the guest node.
IPv6 Address	The IPv6 address of the guest node.
Firmware Version	The version of the firmware operating on the guest node.
HTTP port	The HTTP port as specified with the http-enable command when defining a guest class. You can set this if the guest node provides an HTTP user interface on a non-standard port (any port other than port 80).

Related commands

atmf guest-class

switchport atmf-guestlink

show atmf backup guest

show atmf links

Overview This command displays information about AMF links on a switch. The display output contains link status state information.

Syntax

```
show atmf links [brief]
```

Parameter	Description
`brief`	A brief summary of AMF links, their configuration and status.

Mode User Exec and Privileged Exec

Usage notes The **show atmf links** and **show atmf links brief** commands both produce a table of summarized link information. For a more detailed view use the show atmf links detail command.

This command does not show links that are configured on provisioned ports.

Example To display a brief summary of the AMF links, use the following command:

```
node-1# show atmf links brief
```

Figure 21-26: Example output from **show atmf links brief**

```
Example-core# show atmf links

ATMF Link Brief Information:

Local      Link       Link    ATMF         Adjacent       Adjacent    Link
Port       Type       Status  State        Node           Ifindex     State
-------------------------------------------------------------------------
1.0.10     Crosslink  Down    Init         *crosslink1     -          Blocking
1.0.14     Crosslink  Down    Init         *crosslink2     -          Blocking
1.0.1      Downlink   Down    Init         -               -          Blocking
1.0.2      Downlink   Up      Full         Node2           5001       Forwarding
1.0.8      Downlink   Up      Full         downlink1       5001       Forwarding

* = Provisioned.
```

Table 21-1: Parameter in the output from **show atmf links brief**

Parameter	Definition
`Local Port`	Shows the local port on the selected node.
`Link Type`	Shows link type as Uplink or Downlink (parent and child) or Cross-link (nodes in same domain).
`Link Status`	Shows the link status of the local port on the node as either Up or Down.

Table 21-1: Parameter in the output from **show atmf links brief** (cont.)

Parameter	Definition
ATMF State	Shows AMF state of the local port: • Init - Link is down. • Hold - Link transitioned to up state, but waiting for hold period to ensure link is stable. • Incompatible - Neighbor rejected the link because of inconsistency in AMF configurations. • OneWay - Link is up and has waited the hold down period and now attempting to link to another unit in another domain. • OneWaySim - Device is running in secure mode and link is up but waiting for authorization from an AMF master. • Full - Link hello packets are sent and received from its neighbor with its own node id. • Shutdown - Link has been shut down by user configuration.
Adjacent Node	Shows the Adjacent AMF Node to the one being configured.
Adjacent IF Index	Shows the IF index for the Adjacent AMF Node connected to the node being configured.
Link State	Shows the state of the AMF link. Valid states are either Forwarding or Blocking.

For information on filtering and saving command output, see the "Getting Started with AlliedWare_Plus" Feature Overview and Configuration Guide.

Related commands

no debug all

clear atmf links statistics

show atmf

show atmf links detail

show atmf links guest

show atmf links guest detail

show atmf links statistics

show atmf nodes

show atmf links detail

Overview This command displays detailed information on all the links configured in the AMF network. It can only be run on AMF master and controller nodes.

Syntax

```
show atmf links detail
```

Parameter	Description
`detail`	Detailed AMF links information.

Mode User Exec

Usage notes For summarized link information see the show atmf links command.

This command does not show links that are configured on provisioned ports.

Example To display the AMF link details use this command:

```
device1# show atmf links detail
```

The output from this command will display all the internal data held for AMF links. The following example gives details of the links that are summarized in the example in show atmf links.

Table 22: Sample output from the **show atmf links detail** command

```
device1# show atmf links detail

-------------------------------------------------------------------------------
Crosslink Ports Information
-------------------------------------------------------------------------------
Port                              : sa1
Ifindex                           : 4501
Port Status                       : Down
Port State                        : Init
Last event                        :
Port BPDU Receive Count           : 0
Port                              : po10
Ifindex                           : 4610
Port Status                       : Up
Port State                        : Full
Last event                        : AdjNodeLSEPresent
Port BPDU Receive Count           : 140
Adjacent Node Name                : Building-B
Adjacent Ifindex                  : 4610
Adjacent MAC                      : eccd.6dd1.64d0
Port Last Message Response        : 0
```

Table 22: Sample output from the **show atmf links detail** command (cont.)

```
Port                                : po30
Ifindex                             : 4630
Port Status                         : Up
Port State                          : Full
Last event                          : AdjNodeLSEPresent
Port BPDU Receive Count             : 132
Adjacent Node Name                  : Building-A
Adjacent Ifindex                    : 4630
Adjacent MAC                        : eccd.6daa.c861
Port Last Message Response          : 0

Link State Entries:

Crosslink Ports Blocking            : False
Node.Ifindex                        : Building-A.4630 - Example-core.4630
Transaction ID                      : 2 - 2
MAC Address                         : eccd.6daa.c861 - 0000.cd37.054b
Link State                          : Full - Full

Node.Ifindex                        : Building-B.4610 - Example-core.4610
Transaction ID                      : 2 - 2
MAC Address                         : eccd.6dd1.64d0 - 0000.cd37.054b
Link State                          : Full - Full

Domain Nodes Tree:

Node                                : Building-A
  Links on Node                     : 1
  Link 0                            : Building-A.4630 - Example-core.4630
  Forwarding State                  : Forwarding
Node                                : Building-B
  Links on Node                     : 1
  Link 0                            : Building-B.4610 - Example-core.4610
  Forwarding State                  : Forwarding
Node                                : Example-core
  Links on Node                     : 2
  Link 0                            : Building-A.4630 - Example-core.4630
  Forwarding State                  : Forwarding
  Link 1                            : Building-B.4610 - Example-core.4610
  Forwarding State                  : Forwarding
Crosslink Transaction Entries:

Node                                : Building-B
Transaction ID                      : 2
Uplink Transaction ID               : 6
Node                                : Building-A
Transaction ID                      : 2
Uplink Transaction ID               : 6

Uplink Information:

Waiting for Sync                    : 0
Transaction ID                      : 6
Number of Links                     : 0
Number of Local Uplinks             : 0
```

Table 22: Sample output from the **show atmf links detail** command (cont.)

```
Originating Node                    : Building-A
Domain                              : -'s domain
Node                                : Building-A
Ifindex                             : 0
Node Depth                          : 0
Transaction ID                      : 6
Flags                               : 32
Domain Controller                   : -
Domain Controller MAC               : 0000.0000.0000

Originating Node                    : Building-B
Domain                              : -'s domain
Node                                : Building-B
Ifindex                             : 0
Node Depth                          : 0
Transaction ID                      : 6
Flags                               : 32
Domain Controller                   : -
Domain Controller MAC               : 0000.0000.0000

Downlink Domain Information:

Domain                              : Dept-A's domain
  Domain Controller                 : Dept-A
  Domain Controller MAC             : eccd.6d20.c1d9
  Number of Links                   : 2
  Number of Links Up                : 2
  Number of Links on This Node      : 2
  Links are Blocked                 : 0
  Node Transaction List
    Node                            : Building-B
    Transaction ID                  : 8
    Node                            : Building-A
    Transaction ID                  : 8
  Domain List
    Domain                          : Dept-A's domain
      Node                          : Example-core
      Ifindex                       : 4621
      Transaction ID                : 8
      Flags                         : 1
    Domain                          : Dept-A's domain
      Node                          : Example-core
      Ifindex                       : 4622
      Transaction ID                : 8
      Flags                         : 1
```

Table 22: Sample output from the **show atmf links detail** command (cont.)

```
Domain                              : Dorm-D's domain
  Domain Controller                 : Dorm-D
  Domain Controller MAC             : 0000.cd37.082c
  Number of Links                   : 2
  Number of Links Up                : 2
  Number of Links on This Node      : 2
  Links are Blocked                 : 0
  Node Transaction List
    Node                            : Building-B
    Transaction ID                  : 20
    Node                            : Building-A
    Transaction ID                  : 20
  Domain List
    Domain                          : Dorm-D's domain
      Node                          : Building-A
      Ifindex                       : 0
      Transaction ID                : 20
      Flags                         : 32
    Domain                          : Dorm-D's domain
      Node                          : Building-B
      Ifindex                       : 0
      Transaction ID                : 20
      Flags                         : 32
    Domain                          : Dorm-D's domain
      Node                          : Example-core
      Ifindex                       : 4510
      Transaction ID                : 20
      Flags                         : 1
    Domain                          : Dorm-D's domain
      Node                          : Example-core
      Ifindex                       : 4520
      Transaction ID                : 20
      Flags                         : 1

Domain                              : Example-edge's domain
  Domain Controller                 : Example-edge
  Domain Controller MAC             : 001a.eb93.7aa6
  Number of Links                   : 1
  Number of Links Up                : 1
  Number of Links on This Node      : 0
  Links are Blocked                 : 0
  Node Transaction List
    Node                            : Building-B
    Transaction ID                  : 9
    Node                            : Building-A
    Transaction ID                  : 9
```

Table 22: Sample output from the **show atmf links detail** command (cont.)

```
  Domain List
    Domain                          : Example-edge's domain
      Node                          : Building-A
      Ifindex                       : 0
      Transaction ID                : 9
      Flags                         : 32
    Domain                          : Example-edge's domain
      Node                          : Building-B
      Ifindex                       : 5027
      Transaction ID                : 9
      Flags                         : 1
----------------------------------------------------------------
Up/Downlink Ports Information
----------------------------------------------------------------
Port                                : sa10
Ifindex                             : 4510
Port Status                         : Up
Port State                          : Full
Last event                          : LinkComplete
Adjacent Node                       : Dorm-A
Adjacent Internal ID                : 211
Adjacent Ifindex                    : 4510
Adjacent Board ID                   : 387
Adjacent MAC                        : eccd.6ddf.6cdf
Adjacent Domain Controller          : Dorm-D
Adjacent Domain Controller MAC      : 0000.cd37.082c
Port Forwarding State               : Forwarding
Port BPDU Receive Count             : 95
Port Sequence Number                : 11
Port Adjacent Sequence Number       : 7
Port Last Message Response          : 0
Port                                : po21
Ifindex                             : 4621
Port Status                         : Up
Port State                          : Full
Last event                          : LinkComplete
Adjacent Node                       : Dept-A
Adjacent Internal ID                : 29
Adjacent Ifindex                    : 4621
Adjacent Board ID                   : 340
Adjacent MAC                        : eccd.6d20.c1d9
Adjacent Domain Controller          : Dept-A
Adjacent Domain Controller MAC      : eccd.6d20.c1d9
Port Forwarding State               : Forwarding
Port BPDU Receive Count             : 96
Port Sequence Number                : 8
Port Adjacent Sequence Number       : 9
Port Last Message Response          : 0
Special Link Present                : FALSE
```

Table 23: Parameter definitions from the **show atmf links detail** command output

Parameter	Definition
`Crosslink Ports Information`	Show details of all Crosslink ports on this Node: • Port - Name of the Port or static aggregation (sa<*>). • Ifindex - Interface index for the crosslink port. • VR ID - Virtual router id for the crosslink port. • Port Status - Status of the local port on the Node as UP or DOWN. • Port State - AMF State of the local port. – Init - Link is down. – Hold - Link transitioned to up state, but waiting for hold period to ensure link is stable. – Incompatible - Neighbor rejected the link because of inconsistency in AMF configurations. – OneWay - Link is up and has waited the hold down period and now attempting to link to – another unit in another domain – Full - Link hello packets are sent and received from its neighbor with its own node id. – Shutdown - Link has been shut down by user configuration. Port BPDU Receive Count - The number of AMF protocol PDU's received. • Adjacent Node Name - The name of the adjacent node connected to this node. • Adjacent Ifindex - Adjacent AMF Node connected to this Node. • Adjacent VR ID - Virtual router id of the adjacent node in the domain. • Adjacent MAC - MAC address of the adjacent node in the domain. • Port Last Message Response - Response from the remote neighbor to our AMF last hello packet.
`Link State Entries`	Shows all the link state database entries: • Node.Ifindex - Shows adjacent Node names and Interface index. • Transaction ID - Shows transaction id of the current crosslink transaction. • MAC Address - Shows adjacent Node MAC addresses. • Link State - Shows AMF states of adjacent nodes on the link.
`Domain Nodes Tree`	Shows all the nodes in the domain: • Node - Name of the node in the domain. • Links on Node - Number of crosslinks on a vertex/node. • Link no - Shows adjacent Node names and Interface index. • Forwarding State - Shows state of AMF link Forwarding/Blocking.
`Crosslink Transaction Entries`	Shows all the transaction entries: • Node - Name of the AMF node. • Transaction ID - transaction id of the node. • Uplink Transaction ID - transaction id of the remote node.

Table 23: Parameter definitions from the **show atmf links detail** command output (cont.)

Parameter	Definition
`Uplink Information`	Show all uplink entries. • Waiting for Sync - Flag if uplinks are currently waiting for synchronization. • Transaction ID - Shows transaction id of the local node. • Number of Links - Number of up downlinks in the domain. • Number of Local Uplinks - Number of uplinks on this node to the parent domain. • Originating Node - Node originating the uplink information. • Domain - Name of the parent uplink domain. • Node - Name of the node in the parent domain, that is connected to the current domain. • Ifindex - Interface index of the parent node's link to the current domain. • VR ID - Virtual router id of the parent node's link to the current domain. • Transaction ID - Transaction identifier for the neighbor in crosslink. • Flags - Used in domain messages to exchange the state: ATMF_DOMAIN_FLAG_DOWN = 0 ATMF_DOMAIN_FLAG_UP = 1 ATMF_DOMAIN_FLAG_BLOCK = 2 ATMF_DOMAIN_FLAG_NOT_PRESENT = 4 ATMF_DOMAIN_FLAG_NO_NODE = 8 ATMF_DOMAIN_FLAG_NOT_ACTIVE_PARENT = 16 ATMF_DOMAIN_FLAG_NOT_LINKS = 32 ATMF_DOMAIN_FLAG_NO_CONFIG = 64 • Domain Controller - Domain Controller in the uplink domain • Domain Controller MAC - MAC address of Domain Controller in uplink domain
`Downlink Domain Information`	Shows all the downlink entries: • Domain - Name of the downlink domain. • Domain Controller - Controller of the downlink domain. • Domain Controller MAC - MAC address of the domain controller. • Number of Links - Total number of links to this domain from the Node. • Number of Links Up - Total number of links that are in UP state. • Number of Links on This Node - Number of links terminating on this node. • Links are Blocked - 0 links are not blocked to the domain. 1 All links are blocked to the domain.

Table 23: Parameter definitions from the **show atmf links detail** command output (cont.)

Parameter	Definition
`Node Transaction List`	List of transactions from this downlink domain node. • Node - 0 links are not blocked to the domain. 1 All links are blocked to the domain. • Transaction ID - Transaction id for this node. • Domain List: Shows list of nodes in the current domain and their links to the downlink domain.: • Domain - Domain name of the downlink node. • Node - Name of the node in the current domain. • Ifindex - Interface index for the link from the node to the downlink domain. • Transaction ID - Transaction id of the node in the current domain. • Flags - As mentioned above.
`Up/Downlink Ports Information`	Shows all the configured up and down link ports on this node: • Port - Name of the local port. • Ifindex - Interface index of the local port. • VR ID - Virtual router id for the local port. • Port Status - Shows status of the local port on the Node as UP/DOWN. • Port State - AMF state of the local port. • Adjacent Node - nodename of the adjacent node. • Adjacent Internal ID - Unique node identifier of the remote node. • Adjacent Ifindex - Interface index for the port of adjacent AMF node. • Adjacent Board ID - Product identifier for the adjacent node. • Adjacent VR ID - Virtual router id for the port on adjacent AMF node. • Adjacent MAC - MAC address for the port on adjacent AMF node. • Adjacent Domain Controller - nodename of the Domain controller for Adjacent AMF node. • Adjacent Domain Controller MAC - MAC address of the Domain controller for Adjacent AMF node. • Port Forwarding State - Local port forwarding state Forwarding or Blocking. • Port BPDU Receive Count - count of AMF protocol PDU's received. • Port Sequence Number - hello sequence number, incremented every time the data in the hello packet changes. • Port Adjacent Sequence Number - remote ends sequence number used to check if we need to process this packet or just note it arrived. • Port Last Message Response - response from the remote neighbor to our last hello packet.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Related commands

no debug all

clear atmf links statistics

show atmf

show atmf links guest

Overview This command displays information about guest nodes visible to an AMF device.

Syntax

```
show atmf links guest [interface <interface-range>]
```

Parameter	Description
`interface <interface-range>`	Select a specific range of ports to display information about guest nodes.

Default With no parameters specified this command will display its standard output for all ports with guest nodes connected.

Mode User Exec/Privileged Exec

Usage notes Use this command to display the guest nodes connected to a single parent node. If you want to see a list of all the guests in the AMF network, use show atmf guests.

Example 1 To display information about AMF guests that are connectible from node1, use the command:

```
node1# show atmf links guest
```

Output Figure 21-27: Example output from **show atmf links guest**

```
node1#sh atmf links guest

Guest Link Information:

DC = Discovery configuration
  S = static D = dynamic

Local    Guest         Model        MAC             IP / IPv6
Port     Class         Type      DC Address         Address
-------------------------------------------------------------
1.0.1    -             other     D  0013.1a1e.4589  192.168.1.2
1.0.2    aastra-phone  other     D  0008.5d10.7635  192.168.1.3
1.0.3    cisco-phone2  other     S  -               192.168.2.1
1.0.4    panasonic...  other     D  0800.239e.f1fe  192.168.1.5
```

Table 21-1: Parameters in the output from **show atmf links guest**

Parameter	Description
`Local Port`	The port on the parent node that connects to the guest.
`Guest Class`	The name of the ATMF guest-class that has been assigned to the guest node by the atmf guest-class command.

Table 21-1: Parameters in the output from **show atmf links guest** (cont.)

Parameter	Description
`Model Type`	The model type of the guest node, as entered by the modeltype command. Can be one of the following: • alliedware • aw+ • tq • other
`DC`	The discovery method as applied by the discovery command. This can be either dynamic (D) or static (S).
`MAC Address`	The MAC address of the guest node.
`IP / IPv6 Address`	The IP address of the guest node.

Related commands

atmf guest-class

discovery

http-enable

username (atmf-guest)

modeltype

switchport atmf-guestlink

show atmf backup guest

show atmf links guest detail

Overview This command displays detailed information about guest nodes visible to an AMF device.

Syntax

```
show atmf links guest detail [interface <interface-range>]
```

Parameter	Description
`interface <interface-range>`	Select a specific range of ports to display information about guest nodes.

Mode User Exec and Privileged Exec

Usage notes Use this command to display the guest nodes connected to a single parent node. If you want to see a list of all the guests in the AMF network, use show atmf guests detail.

Note that the parameters that are displayed depend on the guest node's model and state.

Example To display detailed information about AMF guests, use the command:

```
node1# show atmf links guest detail
```

Output Figure 21-28: Example output from **show atmf links guest detail**

```
node1#show atmf links guest detail

Detailed Guest Link Information:

Interface                          : port1.0.13
Link State                         : Down
Class Name                         : test
Model Type                         : Other
Discovery Method                   : Static
IP Address                         : 192.168.1.13
Node State                         : Down

Interface                          : port1.0.5
Link State                         : Full
Class Name                         : tq_device
Model Type                         : TQ
Discovery Method                   : Dynamic
IP Address                         : 192.168.1.221
Username                           : manager
Login Fallback                     : Yes
Node State                         : Full
Backup Supported                   : Yes
MAC address                        : 001a.ebab.d2e0
Device Type                        : AT-TQ4600
Description                        : AP221
Firmware Version                   : 3.2.1 B02
HTTP port                          : 80
```

Table 21-2: Parameters in the output from **show atmf links guest detail**

Parameter	Description
`Interface`	The port on the parent node that connects to the guest.
`Link State`	The state of the link to the guest node; one of: • Down: The physical link is down. • Up: The physical link has come up, but it is still during a timeout period that is enforced to allow other links to come up. • Learn: The timeout period described above has elapsed, and the link is now learning information from the AMF guest node. You can see what information it is learning from the "Node State" field below. • Full: The node connected by this link has joined the AMF network. • Fail: The port is physically up but something has prevented the guest node from joining the AMF network.
`Class Name`	The name of the ATMF guest-class that has been assigned to the guest node by the atmf guest-class command.

Table 21-2: Parameters in the output from **show atmf links guest detail** (cont.)

Parameter	Description
Model Type	The model type of the guest node, as entered by the modeltype command. The mode type can be one of the following: • alliedware • aw+ • onvif • tq • other
Discovery Method	The discovery method as applied by the discovery command. This can be either dynamic or static.
IP Address	The IP address of the guest node.
Username	The user name configured on the guest node.
Login Fallback	Whether the guest node supports Login Fallback. For TQ model guest nodes, when login fallback is enabled, if a guest node is replaced, then AMF logs in to the new TQ using the factory default manager/friend settings. The new TQ is then discovered and managed as an AMF guest node by an AMF master or member. This means any backed up settings for the replaced guest node can also be recovered.
Node state	The state of the guest node; one of: • Down: The initial state when a link to a guest node is first configured. This is also the state if the physical link goes down. • Getting IP: The AMF device is in the process of retrieving the IP address of the guest node. • Getting Mac: The AMF device is in the process of retrieving the MAC address of the guest node. • Getting Info: The AMF device is in the process of retrieving any other available information from the guest (firmware version etc). The information available depends on what device the guest node is. • Full: The AMF device has retrieved all necessary information and the guest node has joined the AMF network. Once this state is reached, the Link State also changes to "Full". • Failure: The physical link is up but the AMF member has failed to retrieve enough information to allow the guest node to join the AMF network.
Backup Supported	Whether the guest node supports AMF backup functionality.
MAC Address	The MAC address of the guest node.

Table 21-2: Parameters in the output from **show atmf links guest detail** (cont.)

Parameter	Description
`Device Type`	Model information for the guest node. This field shows the model information that AMF retrieved from the guest node. In contrast, the Model Type shows what a user entered as the type of device they intended this guest node to be.
`Description`	By default, this is a concatenation of the guest node's parent node and the port to which it is attached. You can change it by configuring a description on the port.
`Serial Number`	The serial number of the guest node.
`Firmware Name`	The name of the firmware operating on the guest node.
`Firmware Version`	The version of the firmware operating on the guest node.
`HTTP port`	The HTTP port as specified with the http-enable command when defining a guest class. You can set this if the guest node provides an HTTP user interface on a non-standard port (any port other than port 80).

Related commands

atmf guest-class

discovery

http-enable

username (atmf-guest)

modeltype

switchport atmf-guestlink

show atmf backup guest

Command changes

Version 5.5.0-1.1: **Login Fallback** parameter added

show atmf links statistics

Overview This command displays details of the AMF links configured on the device and also displays statistics about the AMF packet exchanges between the devices.

It is also possible to display the AMF link configuration and packet exchange statistics for a specified interface.

This command can only be run on AMF master and controller nodes

Syntax `show atmf links statistics [interface [<port-number>]]`

Parameter	Description
`interface`	Specifies that the command applies to a specific interface (port) or range of ports. Where both the interface and port number are unspecified, full statistics (not just those relating to ports will be displayed.
<port-number>	Enter the port number for which statistics are required. A port range, a static channel or LACP link can also be specified. Where no port number is specified, statistics will be displayed for all ports on the device.

Mode User Exec

Example 1 To display AMF link statistics for the whole device, use the command:

```
device1# show atmf links statistics
```

Table 22: Sample output from the **show atmf links statistics** command

```
ATMF Statistics:

                                  Receive        Transmit
------------------------------------------------------------------------------
Arealink Hello                      318            327
Crosslink Hello                     164            167
Crosslink Hello Domain              89             92
Crosslink Hello Uplink              86             88
Hello Link                          0              0
Hello Neighbor                      628            630
Hello Stack                         0              0
Hello Gateway                       1257           1257
Database Description                28             28
Database Request                    8              6
Database Update                     66             162
Database Update Bitmap              0              29
Database Acknowledge                144            51
```

Table 22: Sample output from the **show atmf links statistics** command (cont.)

```
Transmit Fails                          0              1
Discards                                0              0
Total ATMF Packets                      2788           2837

ATMF Database Statistics:

Database Entries                        18
Database Full Ages                      0
ATMF Virtual Link Statistics:

Virtual                                 Receive                    Transmit
link                    Receive         Dropped       Transmit     Dropped
-------------------------------------------------------------------------------
vlink2000               393             0             417          0

ATMF Packet Discards:
Type0   0             : Gateway hello msg received from unexpected neighbor
Type1   0             : Stack hello msg received from unexpected neighbor
Type2   0             : Discard TX update bitmap packet - bad checksum
Type3   0             : Discard TX update packet - neighbor not in correct state
Type4   0             : Discard update packet - bad checksum or type
Type5   0             : Discard update packet - neighbor not in correct state
Type6   0             : Discard update bitmap packet - bad checksum or type
Type7   0             : Incarnation is not possible with the data received
Type8   0             : Discard crosslink hello received - not correct state
Type9   0             : Discard crosslink domain hello received on non crosslink
Type10  0             : Discard crosslink domain hello - not in correct state
Type11  0             : Crosslink uplink hello received on non crosslink port
Type12  0             : Discard crosslink uplink hello - not in correct state
Type13  0             : Wrong network-name for this ATMF
Type14  0             : Packet received on port is too long
Type15  0             : Bad protocol version, received on port
Type16  0             : Bad packet checksum calculation
Type17  0             : Bad authentication type
Type18  0             : Bad simple password
Type19  0             : Unsupported authentication type
Type20  0             : Discard packet - unknown neighbor
Type21  0             : Discard packet - port is shutdown
Type22  0             : Non broadcast hello msg received from unexpected neighbor
Type23  0             : Arealink hello msg received on non arealink port
Type24  0             : Discard arealink hello packet - not in correct state
Type25  0             : Discard arealink hello packet - failed basic processing
Type26  0             : Discard unicast packet - MAC address does not match node
Type27  0             : AMF Master license node limit exceeded
```

Example 2 To display the AMF links statistics on interface port1.0.4, use the command:

```
device1# show atmf links statistics interface port1.0.4
```

Figure 21-29: Sample output from the **show atmf links statistics** command for interface port1.0.4

```
device1# show atmf links statistics interface port1.0.4

ATMF Port Statistics:

                                              Transmit       Receive
-----------------------------------------------------------------------
port1.0.4  Crosslink Hello                      231            232
port1.0.4  Crosslink Hello Domain               116            116
port1.0.4  Crosslink Hello Uplink               116            115
port1.0.4  Hello Link                           0              0
port1.0.4  Arealink Hello                       0              0
```

Figure 21-30: Parameter definitions from the **show atmf links statistics** command output

Parameter	Definition
Receive	Shows a count of AMF protocol packets received per message type.
Transmit	Shows the number of AMF protocol packets transmitted per message type.
Database Entries	Shows the number of AMF elements existing in the distributed database.
Database Full Ages	Shows the number of times the entries aged in the database.
ATMF Packet Discards	Shows the number of discarded packets of each type.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Related commands

no debug all

clear atmf links statistics

show atmf

show atmf nodes

Overview This command displays nodes currently configured within the AMF network.

Note that the output also tells you whether or not node map exchange is active. Node map exchange improves the tracking of nodes joining and leaving an AMF network. This improves the efficiency of AMF networks. Node map exchange is only available if every node in your AMF network is running version 5.4.6-2.1 or later. We recommend running the latest version on all nodes in your network, so you receive the advantages of node map exchange and other improvements.

Syntax

```
show atmf nodes [guest|all]
```

Parameter	Description
`guest`	Display only guest nodes in the AMF network.
`all`	Display all nodes in the AMF network, including guest nodes.

Mode Privileged Exec

Usage notes You can use this command to display one of three sets of nodes:

- all nodes except guest nodes, by specifying **show atmf nodes**
- all nodes including guest nodes, by specifying **show atmf nodes all**
- only guest nodes, by specifying **show atmf nodes guest**

Examples To display AMF information for all nodes except guest nodes, use the command:

```
node1# show atmf nodes
```

Table 21-1: Sample output from **show atmf nodes**

```
node1#show atmf nodes guest

Node Information:

  * = Local device

 SC = Switch Configuration:
  C = Chassis    S = Stackable    N = Standalone

  Node                 Device             ATMF          Parent               Node
  Name                 Type               Master  SC    Domain               Depth
-------------------------------------------------------------------------------
* M1                   x510-28GTX           Y     S     none                   0
  N3                   x230-18GP            N     N     M1                     1
  N1                   AR4050S              N     N     M1                     1

 Node map exchange is active
 Current ATMF node count 3
```

To display AMF information for all nodes, including guest nodes, use the command:

```
node1# show atmf nodes all
```

Table 22: Sample output from **show atmf nodes all**. In this example, not all nodes support node map exchange, as shown by the message at the end

```
node1#show atmf nodes all

 Node and Guest Information:

  * = Local device

 SC = Switch Configuration:
  C = Chassis    S = Stackable    N = Standalone G = Guest

  Node/Guest           Device             ATMF          Parent              Node
  Name                 Type               Master  SC    Domain              Depth
-------------------------------------------------------------------------------
* M1                   x510-28GTX           Y     S     none                  0
  N3                   x230-18GP            N     N     M1                    1
  N1                   AR4050S              N     N     M1                    1
  N3-1.0.24            AT-TQ4600            N     G     N3                    -

Node map exchange is inactive
Firmware on some nodes does not support node map exchange, eg AR4050S
Current ATMF node count 4 (guests 1)
```

To display AMF information for guest nodes only, use the command:

```
node1# show atmf nodes guest
```

Table 21-1: Sample output from **show atmf nodes guest**

```
node1#show atmf nodes guest

Guest Information:
Device        MAC                                      IP/IPv6
Name          Address         Parent            Port   Address
-------------------------------------------------------------------------------
aastra-...    0008.5d10.7635  Node-1            1.0.2  192.168.4.7
poe-1.0.1     0013.1a1e.4589  Node-1            1.0.1  192.168.4.6
ip-camera     0800.239e.f1fe  Node-1            1.0.4  192.168.4.8
tq4600        eccd.6df2.da60  Node-1            1.0.5  192.168.4.50
```

Related commands

show atmf

show atmf area nodes

discovery

http-enable

show atmf backup guest

show atmf provision nodes

Overview This command displays information about each provisioned node with details about date and time of creation, boot and configuration files available in the backup, and license files present in the provisioned backup. This includes nodes that have joined the network but are yet to run their first backup.

This command can only be run on AMF master and controller nodes.

Syntax

```
show atmf provision nodes
```

Mode Privileged Exec

Usage notes This command will only work if provisioned nodes have already been set up. Otherwise, an error message is shown when the command is run.

Example To show the details of all the provisioned nodes in the backup use the command:

```
NodeName# show atmf provision nodes
```

Figure 21-31: Sample output from the **show atmf provision nodes** command

```
device1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media ..............: SD (Total 3827.0MB, Free 3481.1MB)

Node Name                 : device2
Date& Time                : 06-Oct-2016 & 23:25:44
Provision Path            : card:/atmf/provision_nodes

Boot configuration :
Current boot image        : x510-5.4.9-0.1.rel (file exists)
Backup  boot image        : x510-5.4.8-2.3.rel (file exists)
Default boot config       : flash:/default.cfg (file exists)
Current boot config       : flash:/abc.cfg (file exists)
Backup  boot config       : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file           : ./.configs/.sw_v2.lic
                          : ./.configs/.swfeature.lic
Certificate file          : card:/atmf/nodes/awplus1/flash/.atmf-lic-cert
```

Related commands

atmf provision (interface)

atmf provision node

clone (amf-provision)

configure boot config (amf-provision)

configure boot system (amf-provision)

create (amf-provision)

delete (amf-provision)

identity (amf-provision)

license-cert (amf-provision)

locate (amf-provision)

show atmf recovery-file

Overview Use this command to display the recovery file information for an AMF node.

AMF recovery files are created for nodes with special links. Special links include:

- virtual links,
- area links terminating on an AMF master, and
- area virtual links terminating on an AMF master.

Syntax

```
show atmf recovery-file
```

Mode Privileged Exec

Example To display recovery file information for an AMF node, use the command:

```
node1# show atmf recovery-file
```

Output Figure 21-32: Example output from **show atmf recovery-file**

```
node1#show atmf recovery-file

ATMF Recovery File Info: Special Link Present
Location                      Date         Time
USB storage device            30 Apr 2018  14:50:32
Master                        30 Apr 2018  14:56:45
node1                         30 Apr 2018  14:56:45
node3                         30 Apr 2018  14:56:45
```

Related commands

clear atmf recovery-file

show atmf backup

Command changes Version 5.4.8-0.2: command added

show atmf secure-mode

Overview Use this command to display an overview of the secure mode status of an AMF network.

Syntax

```
show atmf secure-mode
```

Mode Privileged Exec

Example To display an overview of AMF secure mode on an AMF master or member node, use the command:

```
awplus# show atmf secure-mode
```

Output Figure 21-33: Example output from **show atmf secure-mode** on an AMF master

```
ATMF Secure Mode:

Secure Mode Status                : Enabled
Certificate Expiry                : 180 Days
Certificates Total                : 8
Certificates Revoked              : 0
Certificates Rejected             : 0
Certificates Active               : 8

Provisional Authorization         : 0
Pending Requests                  : 0

Trusted Master                    : master_1
Trusted Master                    : master_2

Key Fingerprint:
  48:37:d9:a0:37:32:22:9b:5c:22:da:a2:62:49:a7:e5:a9:bc:12:88
```

Figure 21-34: Example output from **show atmf secure-mode** on an AMF node

```
ATMF Secure Mode:

Secure Mode Status                : Enabled
Trusted Master                    : master_1
Trusted Master                    : master_2

Key Fingerprint:
  93:f0:52:a9:74:8f:ae:ea:5b:e2:ee:62:cb:6b:21:22:5a:08:db:98
```

Table 21-2: Parameters in the output from **show atmf secure-mode**

Parameter	Description
`Secure Mode Status`	Shows the status of secure mode, `Enabled` or `Disabled`.
`Certificate Expiry`	Certificate expiry time. Set with atmf secure-mode certificate expiry
`Certificates Total`	Total number of certificates.
`Certificates Revoked`	Certificates that have been revoked by the AMF master.
`Certificates Rejected`	Certificates that have been rejected by the AMF master.
`Certificates Active`	Certificates that are currently active.
`Provisional Authorization`	Number of nodes with provisional authorization. For more information use the show atmf authorization **provisional** command.
`Pending Requests`	Number of nodes waiting for authorization on the AMF master. For more information use the show atmf authorization **pending** command.
`Trusted Master`	List of trusted masters in the AMF area.
`Key Fingerprint`	The AMF node's key fingerprint.

Related commands

atmf authorize

atmf secure-mode

atmf secure-mode certificate expiry

show atmf authorization

show atmf secure-mode audit link

Command changes

Version 5.4.7-0.3: command added

show atmf secure-mode audit

Overview Use this command to detect security vulnerabilities on a node.

Syntax
```
show atmf secure-mode audit
```

Mode Privileged Exec

Example To display AMF secure mode link audits for a node, use the command

```
awplus# show atmf secure-mode audit
```

Output Figure 21-35: Example output from **show atmf secure-mode audit**

```
ATMF Secure Mode Audit:

Warning   : The default username and password is enabled.
Good      : SNMP V1 or V2 is disabled.
Warning   : Telnet server is enabled.
Good      : ATMF is enabled. Secure-Mode is on.
Good      : ATMF Topology-GUI is disabled. No trustpoints configured.

ATMF Secure Mode Log Events:

-------------------------------------------------------------------------
2017 Feb 2 00:59:25 user.notice node1 ATMF[848]: Sec_Audit - ATMF Secure
Mode is enabled.
2017 Feb 2 01:30:00 user.notice node1 ATMF[848]: Sec_Audit - Established
secure connection to area_1_node_1 on interface vlink1.
```

Table 21-3: Parameters in the output from **show atmf secure-mode audit link**

Parameter	Description
`ATMF Secure Mode Audit`	A list of security recommendations to secure the AMF network. Items prefaced with `Warning` need to be fixed. In the sample above the default username and password, and telnet, should be disabled.
`ATMF Secure Mode Log Events`	A list of recorded secure mode log events.

Related commands show atmf secure-mode

Command changes Version 5.4.7-0.3: command added

show atmf secure-mode audit link

Overview Use this command to detect security vulnerabilities by identifying devices that are connected to a secure mode node that are not in secure mode or are not authorized.

Syntax
```
show atmf secure-mode audit link
```

Mode Privileged Exec

Example To display AMF secure mode link audits for a node, use the command

```
awplus# show atmf secure-mode audit link
```

Output Figure 21-36: Example output from **show atmf secure-mode audit link**

```
ATMF Secure Mode Audit Link:

 * ATMF links connected to devices which are not authorized
   or are not in secure-mode.

Port       Link Type  Discovered           Node/Area Name
-----------------------------------------------------------
vlink1     Downlink   16/02/2017 09:28:22  Member3
```

Table 21-4: Parameters in the output from **show atmf secure-mode audit link**

Parameter	Description
Port	Port name on local device.
Link Type	Link type.
Discovered	Date discovered
Node/Area Name	Node or area name of remote device.

Related commands show atmf

show atmf secure-mode

Command changes Version 5.4.7-0.3: command added

show atmf secure-mode certificates

Overview Use this command to display the certificate status details when secure mode is enabled on an AMF network.

Syntax
```
show atmf secure-mode certificates [detail] [area <area-name>]
[node <node-name>]
```

Parameter	Description
`detail`	Display detailed certificate information.
`area`	Specify an AMF area.
<area-name>	The AMF area you want to see the certificate information for.
`node`	Specify an AMF node.
<node-name>	The AMF node you want to see information for.

Mode Privileged Exec

Example To display AMF secure mode certificates on a master or member node, use the command:

```
awplus# show atmf secure-mode certificates
```

To display detailed information about AMF secure mode certificates for a node named “area_2_node_1” in an area named “area-2”, use the command:

```
awplus# show atmf secure-mode certificates detail area area-2
node area_2_node_1
```

Output Figure 21-37: Example output from **show atmf secure-mode certificates**

```
  Area-1 Certificates:
  Node Name             Signer                Expires               Status
------------------------------------------------------------------------------
  area_1_node_1         master_1              11 Mar 2017
                        master_2              4 Mar 2017            Active
  area_1_node_2         master_1              11 Mar 2017
                        master_2              4 Mar 2017            Revoked

  Area-2 Certificates:
  Node Name             Signer                Expires               Status
------------------------------------------------------------------------------
  area_2_node_1         master_1              18 Mar 2017           Active
  area_2_node_2         master_1              18 Mar 2017           Rejected
```

Table 21-5: Parameters in the output from **show atmf secure-mode certificates**

Parameter	Description
`Node Name`	Name of AMF node the certificate was issued to.
`Signer`	Name of AMF master that issued the certificate.
`Expires`	Certificate expiry date.
`Status`	The status column will display `Active` before a member node is trusted, and can be accessed using AMF commands. Valid statuses are `Active`, `Revoked`, and `Rejected`.

Output Figure 21-38: Example output from **show atmf secure-mode certificates detail area area-2 node area_2_node_1**

```
 Certificates Detail:

-------------------------------------------------------------------------------
area_2_node_1 (area:area-2)
  MAC Address     : 0000.cd37.0003
  Status          : Active
  Serial Number   : A24SC8001
  Product         : x510-28GTX
  Key Fingerprint : cd:b4:c9:cd:7b:87:6a:30:98:25:d7:3c:89:8e:cb:74:e8:91:56:9d
  Flags           : 00000011
  Signer          : master_1
  Expiry Date     : 18 Mar 2017 21:17:42
```

Table 21-6: Parameters in the output from **show atmf secure-mode certificates detail**

Parameter	Description
`MAC Address`	MAC address of AMF node.
`Status`	The device status will show `Active` if a member node is trusted, and can be accessed using AMF commands. Valid statuses are `Active`, `Revoked`, and `Rejected`.
`Serial Number`	Device serial number.
`Product`	Device product type.
`Key Fingerprint`	AMF node key fingerprint.
`Flags`	Internal AMF information.
`Signer`	Name of AMF master that issued the certificate.
`Expiry Date`	Certificate expiry date.

Related commands

atmf authorize

atmf secure-mode

atmf secure-mode certificate expire

atmf secure-mode certificate renew

clear atmf secure-mode certificates

show atmf secure-mode sa

Command changes

Version 5.4.7-0.3: command added

show atmf secure-mode sa

Overview Use this command to display the security associations on the network. This is the list of links and neighbors that are trusted.

Syntax

```
show atmf secure-mode sa [detail] [link|neighbor|broadcast]
```

Parameter	Description
`detail`	Display detailed security association information.
`link`	Display security associations for type links.
`neighbor`	Display security associations for type neighbors.
`broadcast`	Display security associations for type broadcast.

Mode Privileged Exec

Example To display an overview of AMF secure mode security associations on a master or member node, use the command:

```
awplus# show atmf secure-mode sa
```

To display a detailed overview of AMF secure mode neighbor security associations on a master or member node, use the command:

```
awplus# show atmf secure-mode sa detail neighbor
```

Output Figure 21-39: Example output from **show atmf secure-mode sa**

```
  ATMF Security Associations:

  Type                        State           ID            Details
-------------------------------------------------------------------------------
  Neighbor Node               Complete        175           master_1
  Broadcast                   Complete        4095
  CrossLink                   Complete        4501          sa1
  AreaLink                    Cert Exchg      4511          sa11
  Link                        Complete        6009          port1.2.9
  AreaLink                    CA Exchg Init   6013          port1.2.13
  AreaLink                    Cert Exchg      13001         port1.9.1
  Link                        CA Exchg Init   16779521      vlink3
  Neighbor Gateway            Complete        83            master_2
  Neighbor Gateway            Complete        175           master_1
  Neighbor Cntl-Master        Complete        83            master_2
  Neighbor Cntl-Master        Complete        175           master_1
```

Figure 21-40: Example output from **show atmf secure-mode sa detail neighbor**

```
 Security Associations Detail:

------------------------------------------------------------
Id                      : 175 (af)
  Type                  : Neighbor Node
  State                 : Complete
  Remote MAC Address    : eccd.6d82.6c16
  Flags                 : 000003c0

Id                      : 83 (40000053)
  Type                  : Neighbor Gateway
  State                 : Complete
  Remote MAC Address    : 001a.eb54.e53b
  Flags                 : 000003c0

Id                      : 175 (400000af)
 Type                   : Neighbor Gateway
 State                  : Complete
 Remote MAC Address     : eccd.6d82.6c16
 Flags                  : 000003c0

Id                      : 83 (80000053)
 Type                   : Neighbor Cntl-Master
 State                  : Complete
 Remote MAC Address     : 001a.eb54.e53b
 Flags                  : 000003c0

Id                      : 175 (800000af)
 Type                   : Neighbor Cntl-Master
 State                  : Complete
 Remote MAC Address     : eccd.6d82.6c16
 Flags                  : 000003c0

Id                      : 321 (80000141)
 Type                   : Neighbor Cntl-Master
 State                  : Complete
 Remote MAC Address     : 0000.f427.93da
 Flags                  : 000003c0
```

Table 21-7: Parameters in the output from **show atmf secure-mode sa**

Parameter	Description
`Type`	Security Association (SA) types: • Link - SA for link • CrossLink - SA for crosslink • AreaLink - SA for area link • Neighbor Node - SA for node neighbor relationship • Neighbor Gateway - SA for gateway neighbor relationship • Neighbor Cntl-Master - SA for controller/master neighbor relationship • Broadcast - SA for working-set broadcast requests
`State`	Current state of the Security Association. The state must be `Complete` before a member node is trusted, and can be accessed using AMF commands. • CA Exchg Init - SA is ready to begin the SA exchange process • CA Exchg - SA is currently exchanging CAs • Cert Exchg - SA is currently exchanging certificates • Key Exchg - SA is currently exchanging ephemeral keys • Complete - SA exchange has completed
`ID`	Security Association ID. • For Neighbor types this is the remote node ID. • For Link types this is the local ifindex. • For Broadcast type this is always 4095.
`Details`	Human readable translation of ID. • For Neighbor types this is the node name • For Link types this is the interface name
`Remote MAC Address`	MAC address of the remote partner of the security association.
`Flags`	Internal AMF information.

Related commands

atmf secure-mode

show atmf secure-mode

show atmf secure-mode certificates

Command changes

Version 5.4.7-0.3: command added

show atmf secure-mode statistics

Overview Use this command to display AMF secure mode statistics. These statistics are from when AMF secure mode was first enabled or the statistics were cleared with the clear atmf secure-mode statistics command.

Syntax
```
show atmf secure-mode statistics
```

Mode Privileged Exec

Example To display AMF secure mode statistics on a master or member node, use the command:

```
awplus# show atmf secure-mode statistics
```

Output Figure 21-41: Example output from **show atmf secure-mode statistics** on an AMF master.

```
ATMF Secure Mode Statistics:

Certificates:
New ............. 7              Expired .......... 0
Updated ......... 7              Deleted .......... 0
Revoked ......... 1              Renewed .......... 2
Rejected ........ 1              Re-authorized .... 1
Authorized ...... 0


Local Certificates:
Valid ........... 4              Invalid  ......... 0
Certificates Validation:
Request Valid ..................................... 2
Request Invalid ................................... 0
Common Valid ...................................... 13
Common Invalid .................................... 0
Issuer Valid ...................................... 14
Issuer Invalid .................................... 0
Signature Verified ................................ 29
Signature Invalid ................................. 0
Signature Purpose Invalid ......................... 0

Signatures Signed ................................. 12
Master Certificates:
Re-issued ......................................... 3
Downgraded to member .............................. 0

Public key change ................................. 2
Invalid SA public key ............................. 0
```

Output Figure 21-42: Example output from **show atmf secure-mode statistics** on an AMF node.

```
ATMF Secure Mode Statistics:


Local Certificates:
Valid ........... 3              Invalid  ......... 0


Certificates Validation:
Request Valid ..................................... 0
Request Invalid ................................... 0
Common Valid ...................................... 0
Common Invalid .................................... 0
Issuer Valid ...................................... 12
Issuer Invalid .................................... 0
Signature Verified ................................ 12
Signature Invalid ................................. 3
Signature Purpose Invalid ......................... 0

Signatures Signed ................................. 0

Master Certificates:
Re-issued ......................................... 0
Downgraded to member .............................. 0

Public key change ................................. 2
Invalid SA public key ............................. 0
```

Related commands

atmf authorize

atmf secure-mode

atmf secure-mode certificate renew

clear atmf secure-mode statistics

show atmf secure-mode

Command changes Version 5.4.7-0.3: command added

show atmf tech

Overview This command collects and displays all the AMF command output. The command can thus be used to display a complete picture of an AMF network.

Syntax

```
show atmf tech
```

Mode Privileged Exec

Example To display output for all AMF commands, use the command:

```
NodeName# show atmf tech
```

Table 22: Sample output from the **show atmf tech** command.

```
node1#show atmf tech
ATMF Summary Information:

ATMF Status            : Enabled
Network Name           : ATMF_NET
Node Name              : node1
Role                   : Master
Current ATMF Nodes     : 8

ATMF Technical information:

Network Name                        : ATMF_NET
Domain                              : node1's domain
Node Depth                          : 0
Domain Flags                        : 0
Authentication Type                 : 0
MAC Address                         : 0014.2299.137d
Board ID                            : 287
Domain State                        : DomainController
Domain Controller                   : node1
Backup Domain Controller            : node2
Domain controller MAC               : 0014.2299.137d
Parent Domain                       : -
Parent Domain Controller            : -
Parent Domain Controller MAC        : 0000.0000.0000
Number of Domain Events             : 0
Crosslink Ports Blocking            : 0
Uplink Ports Waiting on Sync        : 0
```

Table 22: Sample output from the **show atmf tech** command. (cont.)

```
Crosslink Sequence Number          : 7
Domains Sequence Number            : 28
Uplink Sequence Number             : 2
Number of Crosslink Ports          : 1
Number of Domain Nodes             : 2
Number of Neighbors                : 5
Number of Non Broadcast Neighbors  : 3
Number of Link State Entries       : 1
Number of Up Uplinks               : 0
Number of Up Uplinks on This Node  : 0
DBE Checksum                       : 84fc6
Number of DBE Entries              : 0
...
```

Table 23: Parameter definitions from the **show atmf tech** command

Parameter	Definition
ATMF Status	Shows status of AMF feature on the Node as Enabled/Disabled.
Network Name	The name of the AMF network to which this node belongs.
Node Name	The name assigned to the node within the AMF network.
Role	The role configured on the device within the AMF - either master or member.
Current ATMF Nodes	A count of the AMF nodes in the AMF network.
Node Address	The identity of a node (in the format name.atmf) that enables its access it from a remote location.
Node ID	A unique identifier assigned to an AMF node.
Node Depth	The number of nodes in the path from this node to the core domain.
Domain State	A node's state within an AMF Domain - either controller or backup.
Recovery State	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - either Auto, Manual, or None.
Management VLAN	The VLAN created for traffic between nodes of different domains (up/down links). VLAN ID - In this example VLAN 4092 is configured as the Management VLAN. Management Subnet - the Network prefix for the subnet. Management IP Address - the IP address allocated for this traffic. Management Mask - the Netmask used to create a subnet for this traffic 255.255.128.0 (= prefix /17)

Table 23: Parameter definitions from the **show atmf tech** command (cont.)

Parameter	Definition
`Domain VLAN`	The VLAN assigned for traffic between Nodes of same domain (crosslink). VLAN ID - In this example VLAN 4091 is configured as the domain VLAN. Domain Subnet - the Subnet address used for this traffic. Domain IP Address - the IP address allocated for this traffic. 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 node's membership of the core domain (membership is indicated by Y)
`SC`	Shows switch configuration: • C - Chassis (such as SBx8100 series) • S - Stackable (VCS) • N - Standalone
`Parent`	A node that is connected to the present node's uplink, i.e. one layer higher in the hierarchy.
`Node Depth`	Shows the number of nodes in path from the current node to the Core domain.

NOTE: *The **show atmf tech** command can produce very large output. For this reason only the most significant terms are defined in this table.*

show atmf virtual-links

Overview This command displays a summary of all virtual links (L2TP tunnels) currently in the running configuration.

Syntax

```
show atmf virtual-links [macaddr]
show atmf virtual-links [id <1-4094>] [remote-id <1-4094>]
show atmf virtual-links detail [id <1-4094>]
```

Parameter	Description
`macaddr`	Display the virtual AMF links' MAC addresses.
`id <1-4094>`	ID of the local virtual link.
`remote-id <1-4094>`	ID of the remote virtual link
`detail`	Display information about a specific virtual link ID or range of virtual link IDs. Displays information such as: local and remote IP address, link type, packets received and transmitted.

Mode Privileged Exec

Example 1 To display AMF virtual links, use the command:

```
node_1# show atmf virtual-links
```

Table 21-1: Example output from **show atmf virtual-links**

```
ATMF Virtual-Link Information:

Local     Local                Remote               Tunnel    Tunnel
Port      ID   IP              ID   IP              Protect   State
-------------------------------------------------------------------------
vlink1    1    172.16.24.2     2    1.0.0.2         -         Complete
vlink2    2    172.16.24.2*    10   172.16.24.3*    ipsec     Complete
vlink3    3    (eth0)*         1    1.2.3.4         -         AcquireLocal

* = Dynamic Address.

Virtual Links Configured: 3
```

In the above example, a centrally located switch has the IP address space 192.0.2.x/24. It has two VLANs assigned the subnets 192.0.2.33 and 192.0.2.65 using the prefix /27. Each subnet connects to a virtual link. The first link has the IP address 192.168.1.1 and has a Local ID of 1. The second has the IP address 192.168.2.1 and has the Local ID of 2.

Example 2 To display details about AMF virtual link with ID 1, use the command:

```
node_1# show atmf virtual-links detail id 1
```

Table 21-2: Example output from **show atmf virtual-links**

```
  Virtual Link Detailed Information:

  ID 1     Description          : None
  ID 1     Local IP Address     : 192.168.5.1
  ID 1     Remote ID            : 1
  ID 1     Remote IP Address    : 192.168.5.20
  ID 1     Link Type            : virtual-link
  ID 1     Packets Received     : 236465
  ID 1     Packets Transmitted  : 192626
```

Example 3 To display AMF virtual links' MAC address information, use the command:

```
node_1# show atmf virtual-links macaddr
```

Table 21-3: Example output from **show atmf virtual-links macaddr**

```
ATMF Link Remote Information:

ATMF Management Bridge Information:

Bridge: br-atmfmgmt

port no mac addr                is local?       ageing timer
  1     00:00:cd:27:c2:07       yes                0.00
  2     8e:c7:ae:81:7e:68       yes                0.00
  2     00:00:cd:28:bf:e7       no                 0.01
```

Table 21-4: Parameters in the output from **show atmf virtual-links**

Parameter	Definition
Local Port	The tunnel name e.g. vlink1, vlink2, equivalent to an L2TP tunnel.
Local ID	The local ID of the virtual link. This matches the vlink<number>
Tunnel Protect	Tunnel protection protocol.
Tunnel State	The operational state of the vlink (either Up or Down). This state is always displayed once a vlink has been created.
mac addr	AMF virtual links terminate on an internal soft bridge. The "show atmf virtual-links macaddress" command displays MAC Address information.
is local?	Indicates whether the MAC displayed is for a local or a remote device.
ageing timer	Indicates the current aging state for each MAC address.

Related commands atmf virtual-link

show atmf working-set

Overview This command displays the nodes that form the current AMF working-set.

Syntax

```
show atmf working-set
```

Mode Privileged Exec

Example To show current members of the working-set, use the command:

```
ATMF_NETWORK[6]# show atmf working-set
```

Table 22: Sample output from the **show atmf working-set** command.

```
ATMF Working Set Nodes:

node1, node2, node3, node4, node5, node6

Working set contains 6 nodes
```

Related commands

atmf working-set

show atmf

show atmf group

show debugging atmf

Overview Use this command to see what debugging is turned on for AMF.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging atmf
```

Mode Privileged Exec

Example To display the AMF debugging status, use the command:

```
node_1# show debugging atmf
```

Table 21-1: Sample output from the **show debugging atmf** command.

```
node_1# show debugging atmf
ATMF debugging status:
ATMF arealink debugging is on
ATMF link debugging is on
ATMF crosslink debugging is on
ATMF database debugging is on
ATMF neighbor debugging is on
ATMF packet debugging is on
ATMF error debugging is on
```

Related commands debug atmf packet

show debugging atmf packet

Overview Use this command to see what debugging is turned on for AMF Packet debug.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging atmf packet
```

Mode User Exec and Privileged Exec

Example To display the AMF packet debugging status, use the command:

```
node_1# show debug atmf packet
```

Table 21-2: Sample output from the **show debugging atmf packet** command.

```
ATMF packet debugging is on
=== ATMF Packet Debugging Parameters===
Node Name: x908
Port name: port1.1.1
Limit: 500 packets
Direction: TX
Info Level: Level 2
Packet Type Bitmap:
2. Crosslink Hello BPDU pkt with downlink domain info
3. Crosslink Hello BPDU pkt with uplink info
4. Down and up link Hello BPDU pkts
6. Stack hello unicast pkts
8. DBE request
9. DBE update
10. DBE bitmap update
```

Related commands debug atmf

debug atmf packet

show running-config atmf

Overview This command displays the running system information that is specific to AMF.

Syntax
```
show running-config atmf
```

Mode User Exec and Global Configuration

Example To display the current configuration of AMF, use the following commands:

```
node_1# show running-config atmf
```

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Related commands show running-config

no debug all

state

Overview This command sets the running state of an AMF container on a Virtual AMF Appliance (VAA).

An AMF container is an isolated instance of AlliedWare Plus with its own network interfaces, configuration, and file system. The features available inside an AMF container are a sub-set of the features available on the host VAA. These features enable the AMF container to function as a uniquely identifiable AMF master and allows for multiple tenants (up to 60) to run on a single VAA host. See the AMF Feature Overview and Configuration Guide for more information on running multiple tenants on a single VAA host.

Syntax

```
state {enable|disable}
```

Parameter	Description
`disable`	Stop the AMF container. The container's state changes to `stopped`.
`enable`	Start the AMF container. The container's state changes to `running`.

Default By default, **state** is disabled.

Mode AMF Container Configuration

Usage notes The first time the **state enable** command is executed on a container it assigns the container to an area and configures it as an AMF master. This is achieved by automatically adding the following configuration to the AMF container:

```
atmf network-name <AMF network-name>
atmf master
atmf area <container area-name> <container area-id> local
atmf area <container area-name> password <container area-password>
atmf area <host area-name> <host area-id>

interface eth0
 atmf-arealink remote-area <host area-name> vlan 4094
```

For this reason the **state enable** command should be run after the container has been created with the atmf container command and an area-link configured with the area-link command.

Once the start-up configuration has been saved from within the AMF container, all further configuration changes need to be made manually.

Example

To start the AMF container “vac-wlg-1” use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# state enable
```

To stop the AMF container “vac-wlg-1” use the commands:

```
awplus# configure terminal
awplus(config)# atmf container vac-wlg-1
awplus(config-atmf-container)# state disable
```

Related commands

atmf container

show atmf container

Command changes

Version 5.4.7-0.1: command added

switchport atmf-agentlink

Overview Use this command to configure a link between this device and an x600 Series switch, in order to integrate the x600 Series switch into your AMF network. The x600 Series switch is called an "AMF agent", and the link between the x600 and this device is called an "agent link".

The x600 Series switch must be running version 5.4.2-3.16 or later.

Use the **no** variant of this command to remove the agent link. If the x600 Series switch is still connected to the switch port, it will no longer be part of the AMF network.

Syntax

```
switchport atmf-agentlink
no switchport atmf-agentlink
```

Default By default, no agent links exist and x600 Series switches are not visible to AMF networks.

Mode Interface mode for a switch port. Note that the link between the x600 and the AMF network must be a single link, not an aggregated link.

Usage notes The x600 Series switch provides the following information to the AMF node that it is connected to:

- The MAC address
- The IPv4 address
- The IPv6 address
- The name/type of the device (Allied Telesis x600)
- The name of the current firmware
- The version of the current firmware
- The configuration name

AMF guestnode also makes most of this information available from x600 Series switches, but requires configuration with DHCP and/or LLDP. AMF agent is simpler; as soon the x600 is connected to an appropriately configured port of an AMF node, it is immediately integrated into the AMF network.

To see information about the x600 Series switch, use the **show atmf links guest detail** command.

Example To configure port1.0.1 as an agent link, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport atmf-agentlink
```

Related commands show atmf links guest

switchport atmf-arealink

Overview This command enables you to configure a port or aggregator to be an AMF area link. AMF area links are designed to operate between two nodes in different areas in an AMF network.

Use the **no** variant of this command to remove any AMF area link that may exist for the selected port or aggregated link.

This command is only available on AMF controllers and master nodes.

Syntax

```
switchport atmf-arealink remote-area <area-name> vlan <2-4094>
no switchport atmf-arealink
```

Parameter	Description
<area-name>	The name of the remote area that the port is connecting to.
<2-4094>	The VLAN ID for the link. This VLAN cannot be used for any other purpose, and the same VLAN ID must be used at each end of the link.

Default No arealinks are configured.

Mode Interface Configuration for a switchport, a static aggregator, or a dynamic channel group.

Usage notes Run this command on the port or aggregator at both ends of the link.

Each area must have the area-name configured, and the same area password must exist on both ends of the link.

Running this command will automatically place the port or static aggregator into trunk mode (i.e. switchport mode trunk) and will synchronize the area information stored on the two nodes.

You can configure multiple arealinks between two area nodes, but only one arealink at any time will be in use. All other arealinks will block information, to prevent network storms.

NOTE: *See the atmf-arealink command to configure an AMF area link on an AR-series Eth interface.*

Example To make switchport port1.0.2 an arealink to the 'Auckland' area on VLAN 6, use the commands:

```
controller-1# configure terminal
controller-1(config)# interface port1.0.2
controller-1(config-if)# switchport atmf-arealink remote-area
Auckland vlan 6
```

To remove switchport port1.0.1 as an AMF area link, use the commands:

```
controller-1# configure terminal
controller-1(config)# interface port1.0.1
controller-1(config-if)# no switchport atmf-arealink
```

Related commands

atmf area

atmf area password

atmf virtual-link

show atmf links

switchport atmf-crosslink

Overview This command configures the selected port, statically aggregated link or dynamic channel group (LACP) to be an AMF crosslink. Running this command will automatically place the port or aggregator into trunk mode (i.e. **switchport mode trunk**).

The connection between two AMF masters must utilize a crosslink. Crosslinks are used to carry the AMF control information between master nodes. Multiple crosslinks can be configured between two master nodes, but only one crosslink can be active at any particular time. All other crosslinks between masters will be placed in the blocking state, in order to prevent broadcast storms.

Note that AlliedWare Plus CentreCOM Series switches are AMF Edge nodes and do not support virtual links or crosslinks. This is because each edge node can only have a single physical AMF link.

Use the **no** variant of this command to remove any crosslink that may exist for the selected port or aggregated link.

Syntax

```
switchport atmf-crosslink
no switchport atmf-crosslink
```

Mode Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

Usage notes Crosslinks can be used anywhere within an AMF network. They have the effect of separating the AMF network into separate domains.

Example 1 To make switchport port1.0.1 an AMF crosslink, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-crosslink
```

Example 2 This example is shown twice. Example 2A is the most basic command sequence. Example 2B is a good practice equivalent that avoids problems such as broadcast storms that can otherwise occur.

Example 2A To make static aggregator sa1 an AMF crosslink, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface sa1
Node_1(config-if)# switchport atmf-crosslink
```

Example 2B To make static aggregator sa1 an AMF crosslink, use the following commands for good practice:

```
Node_1# configure terminal
Node_1(config)# interface sa1
Node_1(config-if)# switchport atmf-crosslink
Node_1(config-if)# switchport trunk allowed vlan add 2
Node_1(config-if)# switchport trunk native vlan none
```

In this example VLAN 2 is assigned to the static aggregator, and the native VLAN (VLAN 1) is explicitly excluded from the aggregated ports and the crosslink assigned to it.

NOTE: *The AMF management and domain VLANs are automatically added to the aggregator and the crosslink.*

Related commands show atmf links statistics

switchport atmf-guestlink

Overview Guest links are used to provide basic AMF functionality to non AMF capable devices. Guest links can be configured for either a selected switch port or a range of switch ports and use generic protocols to collect status and configuration information that the guest devices make available.

Use the **no** variant of this command to remove the guest node functionality from the selected port or ports.

NOTE: *AMF guest nodes are not supported on ports using the OpenFlow protocol.*

Syntax

```
switchport atmf-guestlink [class <guest-class>] [ip <A.B.C.D>|
ipv6 <X:X::X:X>]
no switchport atmf-guestlink
```

Parameter	Description
`class`	Set a guest class
<guest-class>	The name of the guest class.
`ip`	Specifies that the address following will have an IPv4 format
<A.B.C.D>	The guest node's IP address in IPv4 format.
`ipv6`	Specifies that the address following will have an IPv6 format
<X:X::X:X>	The guest node's IP address in IPv6 format.

Default No guest links are configured.

Mode Interface

Example 1 To configure switchport port1.0.1 to be a guest link, that will connect to a guest node having a guest class of **camera** and an IPv4 address of **192.168.3.3**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink class camera ip
192.168.3.3
```

Example 2 To configure switchport port1.0.1 to be a guest link, which will connect to a guest node having a guest class of **phone** and an IPv6 address of **2001:db8:21e:10d::5**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink class phone ipv6
2000:db8:21e:10d::5
```

Example 3 To configure switchport port1.0.1 to be a guest link, using the default model type and learning method address, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# switchport atmf-guestlink
```

Example 4 To configure switchports port1.0.1 to port1.0.3 to be guest links, for the guest class **camera**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1-port1.0.3
node1(config-if)# switchport atmf-guestlink class camera
```

Example 5 To remove the guest-link functionality from switchport port1.0.1, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.1
node1(config-if)# no switchport atmf-guestlink
```

Related commands

atmf guest-class

discovery

http-enable

username (atmf-guest)

modeltype

show atmf links guest

show atmf guests

switchport atmf-link

Overview This command enables you to configure a port or aggregator to be an up/down AMF link. Running this command will automatically place the port or aggregator into trunk mode. If the port was previously configured in access mode, the configured access VLAN will be removed.

Use the **no** variant of this command to remove any AMF link that may exist for the selected port or aggregated link.

Syntax

```
switchport atmf-link
no switchport atmf-link
```

Mode Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

Usage notes Up/down links and virtual links interconnect domains in a vertical hierarchy, with the highest domain being the core domain. In effect, they form a tree of interconnected AMF domains. This tree must be loop-free. Therefore you must configure your up/down and virtual links so that no loops are formed.

Within each domain, cross-links between AMF nodes define those nodes as siblings within the same domain. You can form rings by combining cross-links with up/down links and/or virtual links, as long as each AMF domain links upwards to only a single parent domain. Each domain may link downwards to multiple child domains.

NOTE: *See the atmf-link command to configure an AMF up/down link on an AR-series Eth interface.*

Example To configure switchport port1.0.1 as an AMF up/down link, use the commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-link
```

To remove switchport port1.0.1 as an AMF up/down link, use the commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# no switchport atmf-link
```

Related commands

atmf-link

show atmf detail

show atmf links

type atmf guest

Overview This command configures a trigger to activate when an AMF guest node joins or leaves.

Syntax

```
type atmf guest {join|leave}
```

Parameter	Description
`join`	AMF guest node joins.
`leave`	AMF guest node leaves.

Mode Trigger Configuration

Example To configure trigger 86 to activate when an AMF guest node leaves, use the following commands:

```
awplus(config)# trigger 86
awplus(config-trigger)# type atmf guest leave
```

Related commands show trigger

Command changes Version 5.5.1-1.1: command added

type atmf node

Overview This command configures a trigger to activate when an AMF node joins or leaves.

Syntax

```
type atmf node {join|leave}
```

Parameter	Description
join	AMF node joins.
leave	AMF node leaves.

Mode Trigger Configuration

Example 1 To configure trigger 5 to activate when an AMF node leaves, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger)# type atmf node leave
```

Example 2 The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
====================
node1, node2, node3:
====================

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=======
node1:
=======

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
001 Periodic (2 min)   Periodic Status Chk  Y  N  Y Continuous  1   smtwtfs
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------

==============
Node2, Node3,
==============

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------
```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
========
Node1:
========

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!

============
Node2, Node3:
============

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

Related commands show trigger

undebug atmf

Overview This command is an alias for the **no** variant of the debug atmf command.

username (atmf-guest)

Overview This command enables you to assign a **username** to a guest class. Guests may require a username and possibly also a password. The password must be between 1 and 32 characters and will allow spaces.

Syntax

```
username <name> password [8] <userpass>
no username
```

Parameter	Description
<name>	User name of the guest node.
8	The parameter **8** means that the password that follows is in hashed form, not plain text. Do not type this 8 when creating a password with this command; it is only used in configuration files. In configuration files, the device prints 8 in front of passwords, to indicate that it is displaying the password in its hashed form.
<userpass>	The password to be entered for the guest node.

Default No usernames are configured

Mode AMF Guest Configuration

Example To assign the user name 'reception' and the password of 'secret' to an AMF guest node that has the guest class of 'phone1' use the following commands:

```
node1# configure terminal
node1(config)# amf guest-class phone1
node1(config-atmf-guest)# username reception password secret
```

To remove a guest node username and password for the user guest class 'phone1', use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class phone1
node1(config-atmf-guest)# no username
```

Related commands

show atmf links detail

atmf guest-class

switchport atmf-guestlink

show atmf links guest

show atmf nodes

22 STOAT Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure Device Discovery using STOAT (Standardized Topology Organizer and Transport).

Using LLDP and DHCP Snooping, STOAT can discover and gather information about devices in the local network. These devices may include IP cameras, IP phones, PCs, laptops, Wi-fi access points, printers, and so on.

Vista Manager EX merges the data from STOAT and existing discovery methods such as AMF, and AMF Plus Device Discovery, to provide a single, accurate and more complete view of the network.

For more information, see the Device Discovery using STOAT Feature Overview and Configuration Guide.

Command List

- "clear stoat collector session counters" on page 824
- "description (stoat-dest)" on page 825
- "key (stoat-dest)" on page 826
- "name-check (stoat-dest)" on page 827
- "service stoat" on page 828
- "show stoat collector" on page 829
- "show stoat destinations" on page 831
- "shutdown (stoat-dest)" on page 833
- "stoat collector enable" on page 834
- "stoat collector expiry-period" on page 835
- "stoat collector key" on page 836
- "stoat collector trustpoint" on page 838
- "stoat destination" on page 839
- "trustpoint (stoat-dest)" on page 841

- "unique-id" on page 842

clear stoat collector session counters

Overview Use this command to clear the STOAT transport session counters.

Syntax

```
clear stoat collector session counters [<1-4294967295>]
```

Parameter	Description
<1-4294967295>	Session ID

Mode Privileged Exec

Example To clear all STOAT transport session counters, use the command:

```
awplus# clear stoat collector session counters
```

To clear a specific STOAT transport session counter, use the command:

```
awplus# clear stoat collector session counters 234234234
```

Related commands

stoat collector trustpoint

show stoat collector

stoat collector expiry-period

stoat collector key

Command changes Version 5.5.3-1.1: command added

description (stoat-dest)

Overview Use this command to add an informative description to a STOAT destination.

Use the **no** variant of this command to remove a description from a STOAT destination.

Syntax

```
description <description>
no description
```

Parameter	Description
<description>	A word or phrase that uniquely identifies this STOAT destination or its purpose. Valid characters are any printable character and spaces, up to a maximum of 40 characters.

Default Not set.

Mode STOAT Destination Configuration

Example To add the description 'chc-collector-1' to a STOAT destination with IP address 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# description chc-collector-1
```

To remove the description from a STOAT destination with IP address 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no description
```

Related commands stoat destination

Command changes Version 5.5.3-1.1: command added

key (stoat-dest)

Overview Use this command to configure a key to use with a STOAT destination. The key allows the STOAT collector to authenticate this device as a valid source. The destination will not attempt to connect if no key is set.

A matching key must be configured on the STOAT collector device.

Use the **no** variant of this command to remove a key for a STOAT destination.

Syntax

```
key [8] <key-string>
no key
```

Parameter	Description
8	Specifies that you are entering a password as a string that has already been encrypted instead of entering a plain text password.The running config displays the new password as an encrypted string even if password encryption is turned off.
<key-string>	Shared key string applied, a value in the range 8 to 80 characters.

Default Not set.

Mode STOAT Destination Configuration

Example To configure the key 'verysecret' for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# key verysecret
```

To remove the key for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no key
```

Related commands stoat collector key

stoat destination

Command changes Version 5.5.3-1.1: command added

name-check (stoat-dest)

Overview Use this command to enable or disable certificate name checking for the server certificate received from the STOAT collector.

Use the **no** variant of this command to disable name checking for the server certificate received from the STOAT collector.

Syntax

```
name-check
no name-check
```

Default Disabled.

Mode STOAT Destination Configuration

Usage notes If enabled, the received server certificate must contain the address configured for this STOAT destination . This setting only takes effect if the STOAT destination has been configured with a trustpoint.

Example To enable name-check for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-destination)# name-check
```

To disable name-check for STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-destination)# no name-check
```

Related commands service stoat

Command changes Version 5.5.3-1.1: command added

service stoat

Overview Use this command to enable or disable Standardized Topology Organizer and Transport (STOAT) functionality on a device. Once enabled, the device will accept STOAT collector and STOAT source configuration.

Use the **no** variant of this command to disable STOAT functionality on a device.

Syntax

```
service stoat
no service stoat
```

Default Disabled.

Mode Global Configuration

Example To enable STOAT functionality on a device, use the commands:

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

To disable STOAT functionality on a device, use the commands:

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

Related commands

stoat collector trustpoint

stoat collector expiry-period

stoat collector key

show stoat collector

Command changes Version 5.5.3-1.1: command added

show stoat collector

Overview Use this command to see the operational status of the STOAT collector.

Syntax

```
show stoat collector [sessions|keys]
```

Parameter	Description
sessions	Active session information
keys	Authentication key information

Mode Privileged Exec

Example To show the STOAT collector status information, use the command:

```
awplus# show stoat collector
```

To show the STOAT collector active session information, use the command:

```
awplus# show stoat collector sessions
```

To show the STOAT collector authentication key information, use the command:

```
awplus# show stoat collector keys
```

Output Figure 22-1: Example output from **show stoat collector**

```
awplus#show stoat collector

STOAT Collector Information:
----------------------------
Status         : Enabled
Expiry-period  : 60 seconds
Trustpoint     : default-selfsigned
```

Figure 22-2: Example output from **show stoat collector sessions**

```
awplus#show stoat collector sessions

STOAT Collector Session Information:
-----------------------------------
Sessions created                        : 2
Sessions expired                        : 0
Sessions failed                         : 0
Sessions failed sync authentication     : 0
Sessions failed update                  : 0
Sessions failed update authentication   : 0

Session ID                              : 3F4B5C27
 Source Name                            : alice
 State                                  : Active
 Counters
  Update success                        : 0
  Update authentication failure         : 0
  Update failure                        : 0
  RX payload bytes                      : 11
  RX payload apteryx set failure        : 0
  RX payload json parse failure         : 0
  RX payload json decode failure        : 0

Session ID                              : 23DFBD7B
 Source Name                            : bob
 State                                  : Active
 Counters
  Update success                        : 0
  Update authentication failure         : 0
  Update failure                        : 0
  RX payload bytes                      : 0
  RX payload apteryx set failure        : 0
  RX payload json parse failure         : 0
  RX payload json decode failure        : 1
```

Figure 22-3: Example output from **show stoat collector keys**

```
awplus#show stoat collector keys

STOAT Collector Key Information:
                                                                  Last Used Time
Key                                          Description            (H:M:S ago)
-------------------------------------------------------------------------------
CoA4E6riSbdWzzetHhHM5F5WdBFPXX2DH6jNzZmYtns=  "generated key"           00:12:52
secret-key                                   "super secret key"              -
```

Related commands

service stoat

stoat collector expiry-period

stoat collector enable

Command changes

Version 5.5.3-1.1: command added

show stoat destinations

Overview Use this command to see the operational status of the configured STOAT destinations.

Syntax

```
show stoat destinations [detail]
```

Parameter	Description
`detail`	Show detailed information

Mode Privileged Exec

Example To show summary information about STOAT destinations, use the command:

```
awplus# show stoat destinations
```

To show detailed information about STOAT destinations, use the command:

```
awplus# show stoat destinations detail
```

Output Figure 22-4: Example output from **show stoat destinations**

```
awplus#show stoat destinations
STOAT Destination Summary Information:
--------------------------------------|
Address      : 192.168.0.12
 State       : Hold

Address      : 192.168.0.2
 State       : Active
```

Figure 22-5: Example output from **show stoat destinations detail**

```
awplus#show stoat destinations detail

STOAT Destination Summary Information:
-------------------------------------|
Address                             : 192.168.0.12
 State                              : Hold
 Session ID                         : 0
 Expiry-period                      : 0 seconds
 Counters:
  Sync OK                           : 0
  Sync failed - unreachable         : 6612
  Sync failed - authentication      : 0
  Sync failed - bad response        : 0
  Update OK                         : 0
  Update failed - unreachable       : 0
  Update failed - authentication    : 0
  Update failed - unknown session   : 0
  RX bytes                          : 0
  TX bytes                          : 0
Address                             : 192.168.0.2
 State                              : Active
 Session ID                         : 200558F4
 Expiry-period                      : 60 seconds
 Counters:
  Sync OK                           : 139
  Sync failed - unreachable         : 10
  Sync failed - authentication      : 0
  Sync failed - bad response        : 0
  Update OK                         : 32773
  Update failed - unreachable       : 52
  Update failed - authentication    : 0
  Update failed - unknown session   : 81
  RX bytes                          : 4099
  TX bytes                          : 16787801
```

Related commands

stoat destination

shutdown (stoat-dest)

Command changes

Version 5.5.3-1.1: command added

shutdown (stoat-dest)

Overview Use this command to disable a STOAT destination.

Use the **no** variant of this command to enable a STOAT destination.

Syntax

```
shutdown
no shutdown
```

Default Enabled (no shutdown)

Mode STOAT Destination Configuration

Example To enable the STOAT destination 192.0.2.6, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no shutdown
```

Related commands stoat destination

show stoat destinations

Command changes Version 5.5.3-1.1: command added

stoat collector enable

Overview Use this command to start or stop the Standardized Topology Organizer and Transport (STOAT) collector functionality on a device.

Note: The device must be able to receive requests from STOAT sources before this command is used. To enable a device to receive requests from STOAT, use the **service stoat** command.

Use the **no** variant of this command to stop the STOAT collector functionality on a device.

Syntax

```
stoat collector enable
no stoat collector enable
```

Default Disabled.

Mode Global Configuration

Usage notes The STOAT feature is responsible for discovering devices and network topology, organizing that information into a standardized format, and transporting it to a central location for use. AMF uses STOAT data to allow non-AMF devices and their links to be displayed in the AMF topology map.

There are two types of STOAT device:

- **Collector** - receives and aggregates topology data
- **Source** - sends data to a collector. The data contains information that it knows about itself and has learned through discovery protocols

Example To start the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector enable
```

To stop the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector enable
```

Related commands

stoat collector trustpoint

show stoat collector

stoat collector expiry-period

stoat collector key

Command changes Version 5.5.3-1.1: command added.

stoat collector expiry-period

Overview Use this command to modify the session expiry-period for all of the STOAT collector's sessions.

Use the **no** variant of this command to revert to the default expiry-period of 60 seconds.

Syntax

```
stoat collector expiry-period <10-300>
no stoat collector expiry-period
```

Parameter	Description
<10-300>	Expiry-period in seconds (default: 60)

Default 60 seconds.

Mode Global Configuration

Example To configure an expiry-period of 15 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector expiry-period 15
```

To revert the expiry-period to its default of 60 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector expiry-period
```

Related commands

service stoat

stoat collector trustpoint

stoat collector key

stoat collector enable

show stoat collector

Command changes Version 5.5.3-1.1: command added

stoat collector key

Overview Use this command to configure the authentication key used by the STOAT collector.

Use the **no** variant of this command to remove a STOAT authentication key.

Syntax

```
stoat collector key [8]{auth-key|generate} [description
<description>]
```

```
no stoat collector key [8]{auth-key|generate} [description
<description>]
```

Parameter	Description
8	Specifies a key in encrypted format instead of plain text.
auth-key	Authentication key
generate	Let STOAT generate a key
description	Add a useful description
<description>	The useful description text

Default Not set.

Mode Global Configuration

Example To configure a plain-text key 'secret-key' with no description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key secret-key
```

To configure a plain-text key 'secret-key' with a description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key secret-key description
'this is my secret key'
```

To **generate** a key with a description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key generate description 'my
generated key'
```

To configure an encrypted key with a description, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector key 8
CFWzNguaqyoPDqYoCBGzff07CfQZOJ-eJO0JslXON3E= description 'my
encrypted key'
```

To remove a configured encrypted key, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector key 8
CFWzNguaqyoPDqYoCBGzff07CfQZOJ-eJO0JslXON3E=
```

Output Figure 22-6: Example output from **stoat collector key generate**

```
awplus(config)# stoat collector key generate

NttWCIS0KsyQ1-1_98qi4HcVdMRykeaE8IKfPe1Xv9o
```

Related commands

service stoat

stoat collector trustpoint

stoat collector expiry-period

stoat collector enable

show stoat collector

Command changes Version 5.5.3-1.1: command added

stoat collector trustpoint

Overview Use this command to add a crypto PKI trustpoint containing a server certificate and a key to the STOAT collector. This enables secure HTTPS API communication between the STOAT collector and STOAT source.

Use the **no** variant of this command to remove a configured PKI trustpoint from a STOAT collector.

Syntax

```
stoat collector trustpoint <trustpoint-name>
no stoat collector trustpoint
```

Parameter	Description
<trustpoint-name>	PKI trustpoint name.

Mode Global Configuration

Example To add an existing PKI trustpoint called 'chc' to the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# stoat collector trustpoint chc
```

To remove a configured PKI trustpoint from the STOAT collector, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat collector trustpoint
```

Related commands

crypto pki authenticate

crypto pki enroll

crypto pki trustpoint

Command changes Version 5.5.3-1.1: command added

stoat destination

Overview Use this command to configure a remote STOAT collector destination.

Use the **no** variant of this command to remove a STOAT collector destination.

Syntax

```
stoat destination {<ip-address>|<host-name>|<ipv6-address>}
no stoat destination {<ip-address>|<host-name>|<ipv6-address>}
```

Parameter	Description
<ip-address>	The IPv4 address, using the format A.B.C.D.
<host-name>	The host name specified in FQDN (Fully Qualified Domain Name). For example, manager.your.domain.com.
<ip6-address>	The IPv6 address, using the format X:X::X:X.

Default Not set.

Mode Global Configuration

Example To configure a remote STOAT collector at IP address 10.0.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 10.0.0.1
```

To remove a remote STOAT collector at IP address 10.0.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat destination 10.0.0.1
```

To configure a remote STOAT collector at stoat.com, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination stoat.com
```

To remove a remote STOAT collector at stoat.com, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat destination stoat.com
```

To configure a remote STOAT collector at 2001:db8 : :1, use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 2001:db8::1
```

To remove a remote STOAT collector at 2001:db8 : :1, use the commands:

```
awplus# configure terminal
awplus(config)# no stoat destination 2001:db8::1
```

Related commands stoat collector key

show stoat collector

Command changes Version 5.5.3-1.1: command added

trustpoint (stoat-dest)

Overview Use this command to specify the trustpoint to use when authenticating the STOAT collector. If no trustpoint is specified, the STOAT collector will be implicitly trusted without authentication.

Use the **no** variant of this command to stop the use of trustpoints with a specified STOAT destination.

Syntax

```
trustpoint <trustpoint-name>
no trustpoint
```

Parameter	Description
<trustpoint-name>	Name of the trustpoint.

Default Not set.

Mode STOAT Destination Configuration

Example To configure the STOAT destination 192.0.2.6 to use trustpoint 'chc', use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# trustpoint chc
```

To stop the use of trustpoints with STOAT destination 192.0.2.6 use the commands:

```
awplus# configure terminal
awplus(config)# stoat destination 192.0.2.6
awplus(config-stoat-dest)# no trustpoint
```

Related commands

stoat collector trustpoint

stoat destination

name-check (stoat-dest)

Command changes Version 5.5.3-1.1: command added

unique-id

Overview Use this command to generate a new unique ID for a device. This ID is used to uniquely identify a device in the STOAT topology.

Some circumstances may require you to generate a new unique ID, for example after recovering a device from an AMF provisioned backup.

Syntax

```
unique-id
```

Mode Privileged Exec

Example To generate a new unique ID for a STOAT device, use the command:

```
awplus# unique-id
```

Related commands service stoat

Command changes Version 5.5.3-1.1: command added

23 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 the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Command List

- "ip address dhcp" on page 844
- "ip dhcp-client default-route distance" on page 846
- "ip dhcp-client request vendor-identifying-specific" on page 848
- "ip dhcp-client vendor-identifying-class" on page 849
- "show counter dhcp-client" on page 850
- "show dhcp lease" on page 851

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
`client-id <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. Default: no default
`hostname <hostname>`	The hostname for the DHCP client on this interface. Typically this name is provided by the ISP. Default: no default

Mode Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

Examples To set the interface eth0 to use DHCP to obtain an IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip address dhcp
```

To stop the interface eth0 from using DHCP to obtain its IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip address dhcp
```

Related commands

ip address (IP Addressing and Protocol)

show ip interface

show running-config

ip dhcp-client default-route distance

Overview Use this command to specify an alternative Administrative Distance (AD) for the current default route (from DHCP) for an interface.

Use the **no** variant of this command to set the AD back to the default of 1.

Syntax

```
ip dhcp-client default-route distance [<1-255>]
no ip dhcp-client default-route distance
```

Parameter	Description
<1-255>	Administrative Distance (AD) from the range 1 though 255.

Default 1

Mode Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

Usage notes DHCP client interfaces can automatically add a default route with an AD of 1 into the IP Routing Information Base (RIB).

Any pre-existing default route(s) via alternative interfaces (configured with a higher AD) will no longer be selected as the preferred forwarding path for traffic when the DHCP based default route is added to the IP routing table.

This can be problematic if the DHCP client is operating via an interface that is only intended to be used for back-up interface redundancy purposes.

Use this command to set the AD of the default route (via a specific DHCP client interface) to a non-default (higher cost) value, ensuring any pre-existing default route(s) via any other interface(s) continue to be selected as the preferred forwarding path for network traffic.

When the command is used, the static default route is deleted from the RIB, the distance value of the route is modified to the configured distance value, then it is reinstalled into the RIB.

Examples To set the AD for the default route added by DHCP via cellular interface eth0 to 150, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-client default-route distance 150
```

To set the AD for the default route back to the default value of 1, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-client default-route distance
```

Related commands

show ip route

show ip route database

Command changes

Version 5.4.7-0.2 Command added.

ip dhcp-client request vendor-identifying-specific

Overview Use this command to add vendor-identifying vendor-specific information (option 125) requests to the DHCP discovery packets sent by an interface. This option, along with option 124, can be used to send vendor-specific information back to a DHCP client.

See RFC3925 for more information on Vendor-Identifying Vendor Options for DHCPv4.

Use the **no** variant of this command to remove the vendor-identifying-specific request from an interface.

Syntax

```
ip dhcp-client request vendor-identifying-specific
no ip dhcp-client request vendor-identifying-specific
```

Default The vendor-identifying-specific request is not configured by default.

Mode Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

Usage notes The DHCP client must be activated on the interface, using the ip address dhcp command, so that DHCP discovery packets are sent.

Example To add the vendor-identifying-specific request on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ip dhcp-client request
vendor-identifying-specific
```

To remove the vendor-identifying-specific request on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-client request
vendor-identifying-specific
```

Related commands ip address dhcp

ip dhcp-client vendor-identifying-class

Command changes Version 5.4.7-2.1: command added

ip dhcp-client vendor-identifying-class

Overview Use this command to add a vendor-identifying vendor class (option 124) to the DHCP discovery packets sent by an interface. This option places the Allied Telesis Enterprise number (207) into the discovery packet. Option 124, along with option 125, can be used to send vendor-specific information back to a DHCP client.

See RFC3925 for more information on Vendor-Identifying Vendor Options for DHCPv4.

Use the **no** variant of this command to remove the vendor-identifying-class from an interface.

Syntax

```
ip dhcp-client vendor-identifying-class
no ip dhcp-client vendor-identifying-class
```

Default The vendor-identifying-class is not configured by default.

Mode Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

Usage notes The DHCP client must be activated on the interface, using the ip address dhcp command, so that DHCP discovery packets are sent.

Example To remove the vendor-identifying-class on eth0, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ip dhcp-client vendor-identifying-class
```

Related commands ip address dhcp

ip dhcp-client request vendor-identifying-specific

Command changes Version 5.4.7-2.1: command added

show counter dhcp-client

Overview This command shows counters for the DHCP client on your device.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show counter dhcp-client
```

Mode User Exec and Privileged Exec

Example To display the message counters for the DHCP client on your device, use the command:

```
awplus# show counter dhcp-client
```

Output Figure 23-1: 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 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 eth0, use the command:

```
awplus# show dhcp lease eth0
```

Output Figure 23-2: Example output from the **show dhcp lease** eth0 command

```
Interface eth0
------------------------------------------------------------------
IP Address:                    192.168.22.4
Expires:                       13 Mar 2022 20:10:19
Renew:                         13 Mar 2022 18:37:06
Rebind:                        13 Mar 2022 19:49:29
Server:
Options:
  subnet-mask                  255.255.255.0
  routers                      19.18.2.100,12.16.2.17
  dhcp-lease-time              3600
  dhcp-message-type            5
  domain-name-servers          192.168.100.50,19.88.200.33
  dhcp-server-identifier       192.168.22.1
  domain-name                  alliedtelesis.com
```

Related commands ip address dhcp

24 DHCP for IPv6 (DHCPv6) Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure DHCPv6. For more information, see the DHCPv6 Feature Overview and Configuration Guide.

DHCPv6 is a network protocol used to configure IPv6 hosts with IPv6 addresses and IPv6 prefixes for an IPv6 network. DHCPv6 is used instead of SLAAC (Stateless Address Autoconfiguration) at sites where centralized management of IPv6 hosts is needed. IPv6 routers require automatic configuration of IPv6 addresses and IPv6 prefixes.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

NOTE: *The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.*

Command List

- "clear counter ipv6 dhcp-client" on page 853
- "clear ipv6 dhcp client" on page 854
- "ipv6 address dhcp" on page 855
- "show counter ipv6 dhcp-client" on page 857
- "show ipv6 dhcp interface" on page 859

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 eth0, use the following command:

```
awplus# clear ipv6 dhcp client eth0
```

ipv6 address dhcp

Overview Use this command to activate the DHCPv6 client on the interface that you are configuring. This allows the interface to use the DHCPv6 client to obtain its IPv6 configuration details from a DHCPv6 server on its connected network.

The command also enables IPv6 on the interface, which creates an EUI-64 link-local address as well as enabling RA processing and SLAAC.

Use the **no** variant of this command to stop the interface from obtaining IPv6 configuration details from a DHCPv6 server.

The DHCPv6 client supports the following IP configuration options:

- Option 1—the subnet mask for your device.
- Option 3—a list of default routers.
- Option 51—lease expiration time.

Syntax

```
ipv6 address dhcp [default-route-to-server]
no ipv6 address dhcp
```

Parameter	Description
`default-route-to-server`	Allow the automatic configuration of a default route to the DHCPv6 server. This option is not enabled by default when you enable the DHCP client on an interface.

Mode Interface Configuration for Eth and bridge interfaces and 802.1Q sub-interfaces.

Usage notes Use the **default-route-to-server** option to allow the automatic configuration of a default route to the DHCPv6 server. Note that this option is not enabled by default when you enable the DHCP client on an interface.

Examples To set the interface eth0 to use DHCPv6 to obtain an IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 address dhcp
```

To stop the interface eth0 from using DHCPv6 to obtain its IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no ipv6 address dhcp
```

Related commands

clear ipv6 dhcp client

ipv6 address

show ipv6 dhcp interface

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 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 24-1: 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 1: Parameters in the output of the **show counter ipv6 dhcp-client** command

Parameter	Description
SOLICIT out	Displays the count of SOLICIT messages sent by the DHCPv6 client.
ADVERTISE in	Displays the count of ADVERTISE messages received by the DHCPv6 client.
REQUEST out	Displays the count of REQUEST messages sent by the DHCPv6 client.
CONFIRM out	Displays the count of CONFIRM messages sent by the DHCPv6 client.
RENEW out	Displays the count of RENEW messages sent by the DHCPv6 client.

Table 1: Parameters in the output of the **show counter ipv6 dhcp-client** command (cont.)

Parameter	Description
`REBIND out`	Displays the count of REBIND messages sent by the DHCPv6 client.
`REPLY in`	Displays the count of REPLY messages received by the DHCPv6 client.
`RELEASE out`	Displays the count of RELEASE messages sent by the DHCPv6 client.
`DECLINE out`	Displays the count of DECLINE messages sent by the DHCPv6 client.
`INFORMATION-REQUEST out`	Displays the count of INFORMATION-REQUEST messages sent by the DHCPv6 client.

show ipv6 dhcp interface

Overview Use this command in User Exec or Privileged Exec mode to display DHCPv6 information for a specified interface, or all interfaces when entered without the interface parameter.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 dhcp interface [<interface-name>]
```

Parameter	Description
<interface-name>	Optional. Specify the name of the interface to show DHCPv6 information about. Omit this optional parameter to display DHCPv6 information for all interfaces DHCPv6 is configured on.

Mode User Exec and Privileged Exec

Example To display DHCPv6 information for all interfaces DHCPv6 is configured on, use the command:

```
awplus# show ipv6 dhcp interface
```

Output Figure 24-2: Example output from the **show ipv6 dhcp interface** command

```
awplus# show ipv6 dhcp interface
eth1 is in client mode
 Address 1001::3c0:1
         preferred lifetime 9000, valid lifetime 5000
         starts  at 20 Jan 2021 09:21:35
         expires at 20 Jan 2021 10:25:32
```

Table 2: Parameters in the output of the **show counter dhcp-client** command

Parameter	Description
Address	Displays the address of the DHCPv6 server on the interface.
Preference	Displays the preference value for the DHCPv6 server.

25 Download Portal Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure Download Portal.

The Download Portal provides a mechanism for administrators to offer resources to network users, protected by authentication. The resources could include software installers and setup guidelines, for example a remote access client along with setup instructions.

For more information, see the Download Portal Feature Overview and Configuration Guide.

Command List

- "aaa authentication download-portal" on page 861
- "download-portal" on page 863
- "download-portal reload" on page 864
- "enable (download-portal)" on page 865
- "file (download-portal)" on page 866
- "http listen" on page 868
- "http secure-listen" on page 870
- "secure-listen (download-portal)" on page 872
- "show download-portal" on page 874
- "uri (download-portal)" on page 875

aaa authentication download-portal

Overview Use this command to globally enable authentication, and set the default authentication method, for Download Portal clients. The default authentication method can be:

- all configured RADIUS servers,
- all configured LDAP servers,
- or a user-defined group of RADIUS or LDAP servers.

Use the **no** variant of this command to globally disable authentication on for Download Portal Clients.

Syntax

```
aaa authentication download-portal default group
[<group-name>|radius|ldap]
```

```
no aaa authentication download-portal default
```

Parameter	Description
<group-name>	Server group name.
radius	Use all RADIUS servers
ldap	Use all LDAP servers

Default Authentication for Download Portal clients is disabled by default.

Mode Global Configuration

Usage notes There are a number of ways to define groups of authentication servers. These are:

- **group radius**: use all RADIUS servers configured with the radius-server host command.
- **group ldap**: use all LDAP servers configured with the ldap-server command.
- **group <group-name>**: use the specified RADIUS or LDAP server group configured with the aaa group server command.

Example To enable LDAP authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authentication download-portal default
group ldap
```

To use a server group to authenticate Download Portal clients, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# aaa authentication download-portal default
group my_group
```

Note: This could be a group of RADIUS or LDAP servers.

To disable authentication for Download Portal clients, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication download-portal default
```

Related commands

aaa group server

download-portal

Command changes

Version 5.5.4-0: command added

download-portal

Overview Use this command to enter Download Portal configuration mode.

Use the **no** variant of this command to remove all Download Portal configuration.

Syntax

```
download-portal
no download-portal
```

Mode Global Configuration

Usage notes The Download Portal enables AlliedWare Plus administrators to provide resources to authenticated network users. These resources may include software installers and setup guidelines, such as a remote access client with accompanying instructions. The resources offered are curated and configured by AlliedWare Plus administrators.

Example To enter Download Portal configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)#
```

To remove all Download Portal configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no download-portal
awplus(config)#
```

Related commands

enable (download-portal)

secure-listen (download-portal)

file (download-portal)

uri (download-portal)

show download-portal

Command changes Version 5.5.4-0: command added

download-portal reload

Overview Use this command to reload the Download Portal which will recreate the Download Portal page.

Syntax

```
download-portal reload
```

Mode Privileged Exec

Usage Notes This is necessary if your device supports external media, such as a USB or SD card, and files are configured from the external media while the external media is not plugged in. When the external media is plugged in the Download Portal page is not automatically reloaded so the files will not appear. Use this command to force a reload.

Example To reload the Download Portal page, use the command:

```
awplus# download-portal reload
```

Related commands download-portal

Command changes Version 5.5.4-0: command added

enable (download-portal)

Overview Use this command to enable the Download Portal.

Use the **no** variant of this command to disable the Download Portal.

Syntax

```
enable
no enable
```

Default Not enabled.

Mode Download Portal Configuration

Example To enable the Download Portal, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# enable
```

To disable the Download Portal, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no enable
```

Related commands download-portal

Command changes Version 5.5.4-0: command added

file (download-portal)

Overview Use this command to configure a file that will be displayed in the Download Portal page.

Use the **no** variant of this command to remove a file from the Download Portal page.

Syntax

```
file <file-path> [sha256sum <hex-string>] [description
<file-description>]
```

```
no file <file-path> [sha256sum <hex-string>] [description
<file-description>]
```

Parameter	Description
<file-path>	The path to the file to be made available in the Download Portal. This file must be present in Flash, USB, or SD card storage.
sha256sum	Optionally, provide the sha256sum of the file. If configured, then this is checked against the file and if it does not match, then it is not displayed on the Download Portal page.
description	Optionally provide a description for the file to be presented to the user accessing the Download Portal page

Mode Download Portal Configuration

Usage notes The file path must be specific, such as starts with "flash:/"(Flash), "usb:/"(USB), or "card:/"(SDcard):

- If the file path is incorrect, the configured file does not show on the Download Portal page.
- The checksum of the file is optional, but if the configured value is not matched, the file will not be shown on the Download Portal page.
- Description is optional, it helps users understand what the file is about.

Example To configure files for the Download Portal page, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# download-portal
```

```
awplus(config-download-portal)# file flash:/staff.txt
sha256sum a1bed1569bef6b9f8958bf8993ef53bf7c2f62a1833fe41f14
description "Staff List"
```

```
awplus(config-download-portal)# file usb:/3g.bin description
"3G file for testing purpose"
```

```
awplus(config-download-portal)# file card:/default.cfg
description "Default Configuration File"
```

To remove a file from the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no file flash:/staff.txt
```

Related commands

download-portal

download-portal reload

Command changes

Version 5.5.4-0: command added

http listen

Overview Use this command to configure the HTTP service to stop listening on all addresses and, instead, listen on a specific address and port.

Use the **no** variant of this command to remove an address and port that the HTTP service was listening on.

Syntax

```
http listen {<ip-address>|<ipv6-address>} <1-65535>
no http listen {<ip-address>|<ipv6-address>} <1-65535>
```

Parameter	Description
<ip-address>	Specify the IPv4 address to listen on for HTTP connections, entered in the form A.B.C.D.
<ipv6-address>	Specify the IPv6 address to listen on for HTTP connections, entered in the form X:X::X:X.
<1-65535>	The TCP port to listen on for HTTP connections.

Mode Privileged Exec

Usage notes AlliedWare Plus devices are configured by default to allow access to the HTTP service using the default HTTP port 80 from any configured address on the device.

However, you can configure the HTTP service to listen on a specific address and port by using the **http listen** command in combination with the **http port none** command. Note, the IP specified must already be configured on the interface that you want to listen on.

These two commands helps to ensure the AlliedWare Plus HTTP service is only reachable on a particular interface. It is recommended that the AlliedWare Plus HTTP service is not accessible from the Internet and/or firewall rules are configured to only allow access from trusted IP networks.

Example To disable the HTTP service listening on all addresses and instead listen on a specific address and port, use the commands:

```
awplus# configure terminal
awplus(config)# http port none
awplus(config)# http listen 192.168.1.1 10080
```

To remove an address and port that the HTTP service was listening on, use the commands:

```
awplus# configure terminal
awplus(config)# no http listen 192.168.1.1 10080
```

Related commands download-portal

Command changes Version 5.5.4-0: command added

http secure-listen

Overview Use this command to configure the HTTPS service to stop listening on all addresses and instead listen on a specific address and port.

Use the **no** variant of this command to remove an address and port that the HTTPS service was listening on.

Syntax

```
http secure-listen {<ip-address>|<ipv6-address>} <1-65535>
no http secure-listen {<ip-address>|<ipv6-address>} <1-65535>
```

Parameter	Description
<ip-address>	Specify the IPv4 address to listen on for HTTPS connections, entered in the form A.B.C.D.
<ipv6-address>	Specify the IPv6 address to listen on for HTTPS connections, entered in the form X:X::X:X.
<1-65535>	The TCP port to listen on for HTTPS connections.

Mode Privileged Exec

Usage notes By default, AlliedWare Plus devices are configured to allow access to the HTTPS service on the default HTTPS port 443 from any configured address on the device.

However, you can configure the HTTPS service to listen on a specific address and port by using the **http secure-listen** command in combination with the **http secure-port none** command. Note, the IP specified must already be configured on the interface that you want to listen on.

These two 'http' commands help ensure the AlliedWare Plus HTTPS service is only reachable on a particular interface. We recommend that the AlliedWare Plus HTTPS service is not accessible from the Internet and/or firewall rules are configured to only allow access from trusted IP networks.

Example To stop the HTTPS service listening on all addresses and instead listen on a specific address and port, use the commands:

```
awplus# configure terminal
awplus(config)# http secure-port none
awplus(config)# http secure-listen 192.168.1.1 10443
```

To remove an address and port that the HTTPS service was listening on, use the commands:

```
awplus# configure terminal
awplus(config)# no http secure-listen 192.168.1.1 10080
```

Related commands download-portal

Command changes Version 5.5.4-0: command added

secure-listen (download-portal)

Overview Use this command to add an address and port for the Download Portal to listen on for HTTPS connections.

Use the **no** variant of this command to remove a secure listen address and port.

Syntax

```
secure-listen {<ip-address>|<ipv6-address>} <1-65535>
no secure-listen {<ip-address>|<ipv6-address>} <1-65535>
```

Parameter	Description
<ip-address>	Specify the IPv4 address to listen on for HTTPS connections, entered in the form A.B.C.D.
<ipv6-address>	Specify the IPv6 address to listen on for HTTPS connections, entered in the form X:X::X:X.
<1-65535>	TCP port to listen on for HTTPS connections.

Mode Download Portal Configuration

Usage notes By default, the Download Portal cannot be accessed because it is not listening on any port for HTTP or HTTPS client connections. The **secure-listen** command must be configured to set the addresses and ports that the Download Portal HTTP service will listen on for clients connections. The IP specified must be configured on an interface.

It is recommended that the firewall rules are configured to ensure that the Download Portal is only reachable by clients that you expect.

Example To add an address and port for the Download Portal to listen on for HTTPS connections, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# secure-listen 192.168.2.45 10443
```

To remove an address and port that the Download Portal was listening on for HTTPS connections, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no secure-listen 192.168.2.45 10443
```

Related commands download-portal

Command changes Version 5.5.4-0: command added

show download-portal

Overview Use this command to show the current status of the Download Portal and display the total configured files and URIs (Uniform Resource Identifiers).

Syntax
```
show download-portal
```

Mode Privileged Exec

Example To show the number of configured URIs and files for the Download Portal, use the command:

```
awplus# show download-portal
```

Output Figure 25-1: Example output from **show download-portal**

```
awplus#show download-portal
Status: Enabled
Files:  2
Secure-listen Addresses:
192.168.1.15:8443
```

Related commands download-portal

Command changes Version 5.5.4-0: command added

uri (download-portal)

Overview Use this command to configure a URI (Uniform Resource Identifier) that links to an external resource to be displayed on the Download Portal page.

Use the **no** variant of this command to remove the URI link from the Download Portal page.

Syntax

```
uri <uri-link> [description <uri-description>]
no uri <uri-link>
```

Parameter	Description
<uri-link>	The URI link to be displayed. It must have a protocol prefix, such as: “https://” or “mailto://”
<uri-description>	Optionally provide a description for the URI to be presented to the user on the Download Portal page.

Mode Download Portal Configuration

Example To set a URI with a description for the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# uri https://alliedtelesis.com
description Company Page
```

To remove a URI for the Download Portal page, use the commands:

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)# no uri
https://alliedtelesis.com
```

Related commands download-portal

Command changes Version 5.5.4-0: command added

26 NTP Commands

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.

The device can act as an NTP client to receive time from one or more NTP servers, and as an NTP server.

For information on filtering and saving command output, see the "Getting Started with AlliedWare_Plus" Feature Overview and Configuration Guide.

Command List

- "ntp authentication-key" on page 877
- "ntp broadcastdelay" on page 878
- "ntp master" on page 879
- "ntp peer" on page 880
- "ntp rate-limit" on page 882
- "ntp restrict" on page 883
- "ntp server" on page 885
- "ntp source" on page 887
- "show ntp associations" on page 889
- "show ntp counters" on page 891
- "show ntp counters associations" on page 892
- "show ntp status" on page 893

ntp authentication-key

Overview This command defines each of the authentication keys. Each key has a key number, a type (MD5 or SHA1), and a value.

The **no** variant of this disables the authentication key.

Syntax

```
ntp authentication-key <keynumber> md5 <key-string> [trusted]
ntp authentication-key <keynumber> sha1 <key-string> [trusted]
no ntp authentication-key <keynumber>
```

Parameter	Description
<keynumber>	*<1-4294967295>* An identification number for the key.
md5	Define an MD5 key.
sha1	Define an SHA1 key.
<key-string>	The authentication key. For SHA1, this is a 20 hexadecimal character string. For MD5, this is a string of up to 31 ASCII characters.
trusted	Add this key to the list of authentication keys that this server trusts.

Mode Global Configuration

Examples To define an MD5 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
```

Command changes Version 5.4.9-2.1 sha1-encrypted parameter added.

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.

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. The default stratum number is 12.

Mode Global Configuration

Usage notes 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

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.

Use the **no** variant of this command to remove the configured NTP peer association.

Syntax

```
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>* Configure the peer authentication key.
`version <version>`	*<1-4>* Configure for this NTP version.

Mode Global Configuration

Examples To set an NTP peer association for this peer with an IPv4 address of 192.0.2.23, use the commands:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.2.23
```

To remove an NTP peer association for this peer with an IPv4 address of 192.0.2.23, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 192.0.2.23
```

To set an NTP peer association for this peer with an IPv6 address of `2001:0db8:010d::1`, use the commands:

```
awplus# configure terminal
awplus(config)# ntp peer 2001:0db8:010d::1
```

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
```

To set the preferred peer to be IPv4 192.0.2.23 and the version to 4, with the authentication key '1234', use the commands:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.2.23 prefer version 4 key 1234
```

Related commands

ntp server

ntp source

ntp rate-limit

Overview Use this command to enable NTP server response rate-limiting. Limiting NTP server responses can reduce network traffic when occurrences such as misconfigured or broken NTP clients poll the NTP server too frequently. Excessive polling can lead to network overload.

Use the **no** variant of this command to remove the rate-limit configuration.

Syntax

```
ntp rate-limit {interval<1-4096>|burst <1-255>|leak <2-16>}
no ntp rate-limit
```

Parameter	Description
`interval`	The minimum interval between responses configured in seconds. The default interval is 8 seconds.
`burst`	The maximum number of responses that can be sent in a burst, temporarily exceeding the limit specified by the interval option. The default burst is 8 responses.
`leak`	The rate at which responses are randomly allowed even if the limits specified by the interval and burst options are exceeded. The default leak is 4, i.e. on average, every fourth request has a response.

Mode Global Configuration

Default Interval - 8 seconds.

Burst - 8 responses.

Leak - 4.

Example To configure an NTP rate-limiting interval of 30 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# ntp rate-limit interval 30
```

Related commands ntp restrict

Command changes Version 5.4.8-1.1: command added

ntp restrict

Overview Use this command to configure a restriction (allow or deny) on NTP packets or NTP functionality for a specific host/network or all hosts of a given IP family.

This means you can control host access to NTP service and NTP server status queries.

Use the **no** variant of this command to remove a restriction from one or more hosts.

Syntax

```
ntp restrict
{default-v4|default-v6|<host-address>|<host-subnet>}
{allow|deny}
```

```
ntp restrict
{default-v4|default-v6|<host-address>|<host-subnet>} query
{allow|deny}
```

```
ntp restrict
{default-v4|default-v6|<host-address>|<host-subnet>} serve
{allow|deny}
```

```
no ntp restrict
{default-v4|default-v6|<host-address>|<host-subnet>}
```

Parameter	Description
`default-v4`	Apply this restriction to all IPv4 hosts.
`default-v6`	Apply this restriction to all IPv6 hosts.
<host-address>	Apply this restriction to the specified IPv4 or IPv6 host. Enter an IPv4 address in the format A.B.C.D. Enter an IPv6 address in the format X:X::X:X.
<host-subnet>	Apply this restriction to the specified IPv4 subnet or IPv6 prefix. Enter an IPv4 subnet in the format A.B.C.D/M. Enter an IPv6 prefix in the format X:X::X:X/X.
`query`	Control NTP server status queries to matching hosts.
`serve`	Control NTP time service to matching hosts.
`allow`	Allow the configured restriction.
`deny`	Deny the configured restriction.

Default By default, time service is allowed to all hosts, and NTP server status querying is denied to all hosts.

Mode Global Configuration

Example

To prevent all IPv4 hosts from accessing a device for NTP service, use the commands:

```
awplus# configure terminal
awplus(config)# ntp restrict default-v4 deny
```

To prevent the host 192.168.1.1 from accessing a device for NTP service, use the commands:

```
awplus# configure terminal
awplus(config)# ntp restrict 198.168.1.1 deny
```

To allow all hosts in the 10.10.10.0/24 subnet to access a device for NTP server status, use the commands:

```
awplus# configure terminal
awplus(config)# ntp restrict 10.10.10.0/24 query allow
```

Related commands

ntp rate-limit

Command changes

Version 5.4.8-1.1: command added

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. You can configure an NTP server association by hostname or IP address.

Use the **no** variant of this command to remove the configured NTP server.

Syntax

```
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>`	Configure the server authentication key from the range 1 to 4294967295.
`version <version>`	Configure for this NTP version from the range 1 to 4.

Mode Global Configuration

Examples To obtain the time by synchronizing with the server at 192.0.1.23, use the commands:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.1.23
```

To obtain the time by synchronizing with the server at 192.0.1.23, and specify that this is the best server to use, use the commands:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.1.23 prefer
```

To obtain the time by synchronizing with the server at 2001:0db8:010e::2, use the commands:

```
awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2
```

To obtain the time by synchronizing with the server at 2001:0db8:010e::2, and specify that this is the best server to use, use the commands:

```
awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2 prefer
```

To stop using the time server at 2001:0db8:010e::2, use the 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.

Note that you cannot use this command when using AMF (Allied Telesis Management Framework).

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 invalid.

Mode Global Configuration

Usage notes 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 is determined by the ntp peer and ntp server commands.

Examples To configure the NTP source interface with the IPv4 address 192.0.2.23, enter the commands:

```
awplus# configure terminal
awplus(config)# ntp source 192.0.2.23
```

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

show ntp associations

Overview Use this command to display the status of NTP associations.

Syntax `show ntp associations`

Mode User Exec and Privileged Exec

Example See the sample output of the **show ntp associations** command displaying the status of NTP associations.

Table 26-1: Example output from **show ntp associations**

```
awplus#show ntp associations
 remote           refid            st t when poll reach    delay   offset  disp
------------------------------------------------------------------------------
*server1.example.com
                 192.0.2.2        4 u   47   64   377    0.177    0.021   0.001
+192.168.1.10    10.32.16.80      5 u   46   64   377    0.241   -0.045   0.000
* system peer, # backup, + candidate, - outlier, x false ticker
```

Table 26-2: Parameters in the output from **show ntp associations**

Parameter	Description
`* system peer`	The peer that NTP uses to calculate variables like the offset and root dispersion of this AlliedWare Plus device. NTP passes these variables to the clients using this AlliedWare Plus device.
`# backup`	Peers that are usable, but are not among the first six peers sorted by synchronization distance. These peers may not be used.
`+ candidate`	Peers that the NTP algorithm has determined can be used, along with the system peer, to discipline the clock (i.e. to set the time on the AlliedWare Plus device).
`- outlier`	Peers that are not used because their time is significantly different from the other peers.
`x false ticker`	Peers that are not used because they are not consider trustworthy.
`space`	Peers that are not used because they are, for example, unreachable.
`remote`	The peer IP address
`refid`	The IP address of the reference clock, or an abbreviation indicating the type of clock (e.g. GPS indicates that the server uses GPS for the reference clock). INIT indicates that the reference clock is initializing, so it is not operational.

Table 26-2: Parameters in the output from **show ntp associations** (cont.)

Parameter	Description
st	The stratum, which is the number of hops between the server and the accurate time source such as an atomic clock.
t	Type, one of: u: unicast or manycast client b: broadcast or multicast clientl: local reference clock s: symmetric peer A: manycast server B: broadcast server M: multicast server
when	When last polled (seconds ago, h hours ago, or d days ago).
poll	Time between NTP requests from the device to the server.
reach	An indication of whether or not the NTP server is responding to requests. 0 indicates there has never been a successful poll; 1 indicates that the last poll was successful; 3 indicates that the last two polls were successful; 377 indicates that the last 8 polls were successful.
delay	The round trip communication delay to the remote peer or server, in milliseconds.
offset	The mean offset (phase) in the times reported between this local host and the remote peer or server (root mean square, milliseconds).
disp	The amount of clock error (in milliseconds) of the server due to clock resolution, network congestion, etc.

show ntp counters

Overview This command displays packet counters for NTP.

Syntax

```
show ntp counters
```

Mode Privileged Exec

Example To display counters for NTP use the command:

```
awplus# show ntp counters
```

Figure 26-1: Example output from **show ntp counters**

```
awplus#show ntp counters
Server Received           4
Server Dropped            0
Client Sent               90
Client Received           76
Client Valid Received     76
```

Table 26-3: Parameters in the output from **show ntp counters**

Parameter	Description
`Server Received`	Number of NTP packets received from NTP clients.
`Server Dropped`	Number of NTP packets received from NTP clients but dropped.
`Client Sent`	Number of NTP packets sent to servers.
`Client Received`	Number of NTP packets received from servers
`Client Valid Received`	Number of valid NTP packets received from servers.

show ntp counters associations

Overview Use this command to display NTP packet counters for individual servers and peers.

Syntax

```
show ntp counters associations
```

Mode Privileged Exec

Examples To display packet counters for each NTP server and peer that is associated with a device, use the command:

```
awplus# show ntp counters associations
```

Output Figure 26-2: Example output from **show ntp counters associations**

```
awplus#show ntp counters associations
Peer 2001::1
 sent:          -
 received:      -
Peer 10.37.219.100
 sent:          7
 received:      7
```

Table 26-4: Parameters in the output from **show ntp counters associations**

Parameter	Description
Peer	An NTP peer or server that the device is associated with.
sent	The number of NTP packets that this device sent to the peer.
received	The number of NTP packets that this device received from the peer.

Related commands ntp restrict

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 To see information about NTP status, use the command:

```
awplus# show ntp status
```

For information about the output displayed by this command, see ntp.org.

Figure 26-3: Example output from **show ntp status**

```
awplus#show ntp status
Reference ID    : C0A8010A (192.168.1.10)
Stratum         : 4
Ref time (UTC)  : Fri Jun 15 05:32:38 2018
System time     : 0.000002004 seconds fast of NTP time
Last offset     : -0.002578615 seconds
RMS offset      : 0.000928071 seconds
Frequency       : 5.099 ppm slow
Residual freq   : -9.120 ppm
Skew            : 17.486 ppm
Precision       : -21 (0.000000477 seconds)
Root delay      : 0.031749818 seconds
Root dispersion : 0.133974627 seconds
Update interval : 65.3 seconds
Leap status     : Normal
```

27 SNMP Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure SNMP. For more information, see:

- the Support for Allied Telesis Enterprise_MIBs in AlliedWare Plus, for information about which MIB objects are supported.
- the SNMP Feature Overview and Configuration_Guide.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Command List

- "alias (interface)" on page 896
- "debug snmp" on page 897
- "show counter snmp-server" on page 898
- "show debugging snmp" on page 902
- "show running-config snmp" on page 903
- "show snmp-server" on page 904
- "show snmp-server community" on page 905
- "show snmp-server group" on page 906
- "show snmp-server trap" on page 907
- "show snmp-server user" on page 908
- "show snmp-server view" on page 909
- "snmp trap link-status" on page 910
- "snmp trap link-status suppress" on page 911
- "snmp-server" on page 913
- "snmp-server community" on page 915
- "snmp-server contact" on page 916

- "snmp-server enable trap" on page 917
- "snmp-server engineID local" on page 920
- "snmp-server engineID local reset" on page 922
- "snmp-server group" on page 923
- "snmp-server host" on page 925
- "snmp-server legacy-ifadminstatus" on page 927
- "snmp-server location" on page 928
- "snmp-server source-interface" on page 929
- "snmp-server startup-trap-delay" on page 930
- "snmp-server user" on page 931
- "snmp-server view" on page 934
- "undebug snmp" on page 935

alias (interface)

Overview Use this command to set an alias name for a port, as returned by the SNMP ifMIB in OID 1.3.6.1.2.1.31.1.1.1.18.

Use the **no** variant of this command to remove an alias name from a port.

Syntax

```
alias <ifAlias>
no alias
```

Parameter	Description
<ifAlias>	64 character name for an interface in a network management system. All printable characters are valid.

Default Not set.

Mode Interface Configuration

Usage notes The interface alias can also be set via SNMP.

Third-party management systems often use standard MIBs to access device information. Network managers can specify an alias interface name to provide a non-volatile way to access the interface.

Example To configure the alias interface name 'uplink_a' for eth0, use the following commands:

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

To remove an alias interface name from eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no alias
```

Command changes Version 5.4.8-2.1: command added

debug snmp

Overview This command enables SNMP debugging.

The **no** variant of this command disables SNMP debugging.

Syntax

```
debug snmp
[all|detail|error-string|process|receive|send|xdump]
```

```
no debug snmp
[all|detail|error-string|process|receive|send|xdump]
```

Parameter	Description
`all`	Enable or disable the display of all SNMP debugging information.
`detail`	Enable or disable the display of detailed SNMP debugging information.
`error-string`	Enable or disable the display of debugging information for SNMP error strings.
`process`	Enable or disable the display of debugging information for processed SNMP packets.
`receive`	Enable or disable the display of debugging information for received SNMP packets.
`send`	Enable or disable the display of debugging information for sent SNMP packets.
`xdump`	Enable or disable the display of hexadecimal dump debugging information for SNMP packets.

Mode Privileged Exec and Global Configuration

Example To start SNMP debugging, use the command:

```
awplus# debug snmp
```

To start SNMP debugging, showing detailed SNMP debugging information, use the command:

```
awplus# debug snmp detail
```

To start SNMP debugging, showing all SNMP debugging information, use the command:

```
awplus# debug snmp all
```

Related commands

show debugging snmp

terminal monitor

undebug snmp

show counter snmp-server

Overview This command displays counters for SNMP messages received by the SNMP agent.

Syntax

```
show counter snmp-server
```

Mode User Exec and Privileged Exec

Example To display the counters for the SNMP agent, use the command:

```
awplus# show counter snmp-server
```

Output Figure 27-1: Example output from the **show counter snmp-server** command

```
SNMP-SERVER counters
inPkts                ......... 11
inBadVersions         ......... 0
inBadCommunityNames   ......... 0
inBadCommunityUses    ......... 0
inASNParseErrs        ......... 0
inTooBigs             ......... 0
inNoSuchNames         ......... 0
inBadValues           ......... 0
inReadOnlys           ......... 0
inGenErrs             ......... 0
inTotalReqVars        ......... 9
inTotalSetVars        ......... 0
inGetRequests         ......... 2
inGetNexts            ......... 9
inSetRequests         ......... 0
inGetResponses        ......... 0
inTraps               ......... 0
outPkts               ......... 11
outTooBigs            ......... 0
outNoSuchNames        ......... 2
outBadValues          ......... 0
outGenErrs            ......... 0
outGetRequests        ......... 0
outGetNexts           ......... 0
outSetRequests        ......... 0
outGetResponses       ......... 11
outTraps              ......... 0
UnSupportedSecLevels  ......... 0
NotInTimeWindows      ......... 0
UnknownUserNames      ......... 0
UnknownEngineIDs      ......... 0
WrongDigest           ......... 0
DecryptionErrors      ......... 0
UnknownSecModels      ......... 0
InvalidMsgs           ......... 0
UnknownPDUHandlers    ......... 0
```

Table 1: Parameters in the output of the **show counter snmp-server** command

Parameter	Meaning
inPkts	The total number of SNMP messages received by the SNMP agent.
inBadVersions	The number of messages received by the SNMP agent for an unsupported SNMP version. It drops these messages.The SNMP agent on your device supports versions 1, 2C, and 3.
inBadCommunityNames	The number of messages received by the SNMP agent with an unrecognized SNMP community name. It drops these messages.
inBadCommunityUses	The number of messages received by the SNMP agent where the requested SNMP operation is not permitted from SNMP managers using the SNMP community named in the message.
inASNParseErrs	The number of ASN.1 or BER errors that the SNMP agent has encountered when decoding received SNMP Messages.
inTooBigs	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'tooBig'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inNoSuchNames	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'noSuchName'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inBadValues	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'badValue'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inReadOnlys	The number of valid SNMP PDUs received by the SNMP agent where the value of the error-status field is 'readOnly'. The SNMP manager should not generate a PDU which contains the value 'readOnly' in the error-status field. This indicates that there is an incorrect implementations of the SNMP.
inGenErrs	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'genErr'.

Table 1: Parameters in the output of the **show counter snmp-server** command

Parameter	Meaning
inTotalReqVars	The number of MIB objects that the SNMP agent has successfully retrieved after receiving valid SNMP Get-Request and Get-Next PDUs.
inTotalSetVars	The number of MIB objects that the SNMP agent has successfully altered after receiving valid SNMP Set-Request PDUs.
inGetRequests	The number of SNMP Get-Request PDUs that the SNMP agent has accepted and processed.
inGetNexts	The number of SNMP Get-Next PDUs that the SNMP agent has accepted and processed.
inSetRequests	The number of SNMP Set-Request PDUs that the SNMP agent has accepted and processed.
inGetResponses	The number of SNMP Get-Response PDUs that the SNMP agent has accepted and processed.
inTraps	The number of SNMP Trap PDUs that the SNMP agent has accepted and processed.
outPkts	The number of SNMP Messages that the SNMP agent has sent.
outTooBigs	The number of SNMP PDUs that the SNMP agent has generated with the value 'tooBig' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outNoSuchNames	The number of SNMP PDUs that the SNMP agent has generated with the value `noSuchName' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outBadValues	The number of SNMP PDUs that the SNMP agent has generated with the value 'badValue' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outGenErrs	The number of SNMP PDUs that the SNMP agent has generated with the value 'genErr' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outGetRequests	The number of SNMP Get-Request PDUs that the SNMP agent has generated.

Table 1: Parameters in the output of the **show counter snmp-server** command

Parameter	Meaning
outGetNexts	The number of SNMP Get-Next PDUs that the SNMP agent has generated.
outSetRequests	The number of SNMP Set-Request PDUs that the SNMP agent has generated.
outGetResponses	The number of SNMP Get-Response PDUs that the SNMP agent has generated.
outTraps	The number of SNMP Trap PDUs that the SNMP agent has generated.
UnSupportedSecLevels	The number of received packets that the SNMP agent has dropped because they requested a securityLevel unknown or not available to the SNMP agent.
NotInTimeWindows	The number of received packets that the SNMP agent has dropped because they appeared outside of the authoritative SNMP agent's window.
UnknownUserNames	The number of received packets that the SNMP agent has dropped because they referenced an unknown user.
UnknownEngineIDs	The number of received packets that the SNMP agent has dropped because they referenced an unknown snmpEngineID.
WrongDigest	The number of received packets that the SNMP agent has dropped because they didn't contain the expected digest value.
DecryptionErrors	The number of received packets that the SNMP agent has dropped because they could not be decrypted.
UnknownSecModels	The number of messages received that contain a security model that is not supported by the server. Valid for SNMPv3 messages only.
InvalidMsgs	The number of messages received where the security model is supported but the authentication fails. Valid for SNMPv3 messages only.
UnknownPDUHandlers	The number of times the SNMP handler has failed to process a PDU. This is a system debugging counter.

Related commands show snmp-server

show debugging snmp

Overview This command displays whether SNMP debugging is enabled or disabled.

Syntax

```
show debugging snmp
```

Mode User Exec and Privileged Exec

Example To display the status of SNMP debugging, use the command:

```
awplus# show debugging snmp
```

Output Figure 27-2: Example output from the **show debugging snmp** command

```
Snmp (SMUX) debugging status:
  Snmp 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 27-3: 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 27-4: 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 27-5: 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 27-6: Example output from the **show snmp-server group** command

```
SNMP group information:
  Group name ............... guireadgroup
    Security Level ........ priv
    Read View ............. guiview
    Write View ............ none
    Notify View ........... none

  Group name ............... guiwritegroup
    Security Level ........ priv
    Read View ............. none
    Write View ............ guiview
    Notify View ........... none
```

Related commands show snmp-server

snmp-server group

show snmp-server trap

Overview Use this command to display the status of the SNMP traps.

Syntax

```
show snmp-server trap
```

Mode Privileged Exec

Example To display the SNMP traps status, use the commands:

```
awplus# show snmp-server trap
```

Output Figure 27-7: Example output from **show snmp-server trap**

```
awplus#show snmp-server trap
ATMF traps ............................ Disabled
ATMF Link traps ....................... Disabled
ATMF Node traps ....................... Disabled
ATMF Guest Node traps ................. Enabled
ATMF Reboot Rolling traps ............. Disabled
Authentication failure ................ Disabled
BGP traps ............................. Disabled
CWM Access Point traps ................ Enabled
DHCP Snooping traps ................... Disabled
EPSR traps ............................ Disabled
LLDP traps ............................ Disabled
Loop Protection traps ................. Disabled
MSTP traps ............................ Disabled
NSM traps ............................. Disabled
OSPF traps ............................ Disabled
PIM traps ............................. Disabled
Power-inline traps .................... Disabled
QoS Storm Protection traps ............ Enabled
RMON traps ............................ Disabled
MAC address Thrash Limiting traps .... Disabled
UDLD traps ............................ Disabled
VCS traps ............................. Disabled
VRRP traps ............................ Disabled
Wireless traps ........................ Disabled
```

Related commands

show snmp-server

snmp-server enable trap

show snmp-server user

Overview This command displays the SNMP server users and is used with SNMP version 3 only.

Syntax
```
show snmp-server user
```

Mode Privileged Exec

Example To display the SNMP server users configured on the device, use the command:

```
awplus# show snmp-server user
```

Output Figure 27-8: Example output from the **show snmp-server user** command

```
Name                Group name          Auth        Privacy
-------             -------------       -------     ----------
freddy              guireadgroup        none        none
```

Related commands
show snmp-server

snmp-server user

show snmp-server view

Overview This command displays the SNMP server views and is used with SNMP version 3 only.

Syntax
```
show snmp-server view
```

Mode Privileged Exec

Example To display the SNMP server views configured on the device, use the command:

```
awplus# show snmp-server view
```

Output Figure 27-9: Example output from the **show snmp-server view** command

```
SNMP view information:
  View Name ............... view1
    OID ..................... 1
    Type .................... included
```

Related commands
show snmp-server

snmp-server view

snmp trap link-status

Overview Use this command to enable SNMP to send link status notifications (traps) for the interfaces when an interface goes up (linkUp) or down (linkDown).

Use the **no** variant of this command to disable the sending of link status notifications.

Syntax

```
snmp trap link-status [enterprise]
no snmp trap link-status
```

Parameter	Description
`enterprise`	Send an Allied Telesis enterprise type of link trap.

Default Disabled

Mode Interface Configuration

Usage notes The link status notifications can be enabled for the following interface types:

- Ethernet (e.g. eth0)

To specify where notifications are sent, use the snmp-server host command. To configure the device globally to send other notifications, use the snmp-server enable trap command.

Examples To enable SNMP to send link status notifications for eth0 use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# snmp trap link-status
```

To disable the sending of link status notifications for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no snmp trap link-status
```

Related commands

show interface

snmp trap link-status suppress

snmp-server enable trap

snmp-server host

snmp trap link-status suppress

Overview Use this command to enable the suppression of link status notifications (traps) for the interfaces beyond the specified threshold, in the specified interval.

Use the **no** variant of this command to disable the suppression of link status notifications for the ports.

Syntax

```
snmp trap link-status suppress {time {<1-60>|default}|threshold
{<1-20>|default}}
```

```
no snmp trap link-status suppress
```

Parameter	Description
`time`	Set the suppression timer for link status notifications.
<1-60>	The suppress time in seconds.
`default`	The default suppress time in seconds (60).
`threshold`	Set the suppression threshold for link status notifications. This is the number of link status notifications after which to suppress further notifications within the suppression timer interval.
<1-20>	The number of link status notifications.
`default`	The default number of link status notifications (20).

Default By default, if link status notifications are enabled (they are enabled by default), the suppression of link status notifications is enabled: notifications that exceed the notification threshold (default 20) within the notification timer interval (default 60 seconds) are not sent.

Mode Interface Configuration

Usage notes An unstable network can generate many link status notifications. When notification suppression is enabled, a suppression timer is started when the first link status notification of a particular type (linkUp or linkDown) is sent for an interface.

If the threshold number of notifications of this type is sent before the timer reaches the suppress time, any further notifications of this type generated for the interface during the interval are not sent. At the end of the interval, the sending of link status notifications resumes, until the threshold is reached in the next interval.

Examples To suppress link- status notifications for eth0 after 10 notifications in 40 seconds, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# interface eth0
```

```
awplus(config-if)# snmp trap link-status suppress time 40
threshold 10
```

To stop suppressing link status notifications for eth0, use the following commands:

```
awplus# configure terminal
awplus(config)# interface eth0
awplus(config-if)# no snmp trap link-status suppress
```

Related commands

show interface

snmp trap link-status

snmp-server

Overview Use this command to enable the SNMP agent (server) on the device. The SNMP agent receives and processes SNMP packets sent to the device, and generates notifications (traps) that have been enabled by the snmp-server enable trap command.

Use the **no** variant of this command to disable the SNMP agent on the device. When SNMP is disabled, SNMP packets received by the device are discarded, and no notifications are generated. This does not remove any existing SNMP configuration.

Syntax

```
snmp-server [ip|ipv6]
no snmp-server [ip|ipv6]
```

Parameter	Description
ip	Enable or disable the SNMP agent for IPv4.
ipv6	Enable or disable the SNMP agent for IPv6.

Default By default, the SNMP agent is enabled for both IPv4 and IPv6. If neither the **ip** parameter nor the **ipv6** parameter is specified for this command, then SNMP is enabled or disabled for both IPv4 and IPv6.

Mode Global Configuration

Examples To enable SNMP on the device for both IPv4 and IPv6, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server
```

To enable the SNMP agent for IPv4 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server ip
```

To disable the SNMP agent for both IPv4 and IPv6 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-server
```

To disable the SNMP agent for IPv4, use the commands:

```
awplus(config)# no snmp-server ipv4
```

Related commands

show snmp-server

show snmp-server community

show snmp-server user

snmp-server community

snmp-server contact

snmp-server enable trap

snmp-server engineID local

snmp-server group

snmp-server host

snmp-server location

snmp-server view

snmp-server community

Overview This command creates an SNMP community, optionally setting the access mode for the community. The default access mode is read-only. If the view parameter is not specified, the community allows access to all the MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used when operating SNMPv3.

The **no** variant of this command removes an SNMP community. The specified community must already exist on the device.

Syntax

```
snmp-server community <community-name> [view <view-name>|ro|rw]
no snmp-server community <community-name>
```

Parameter	Description
<community-name>	Community name. The community name is a case sensitive string of up to 20 characters.
`view`	Configure SNMP view. If view is not specified, the community allows access to all the MIB objects.
<view-name>	View name. The view name is a string up to 20 characters long and is case sensitive.
`ro`	Read-only community.
`rw`	Read-write community.

Default The default access mode is Read-only.

Mode Global Configuration

Example Use the following commands to create an SNMP community called 'public' with read-only access to all MIB variables from any management station:

```
awplus# configure terminal
awplus(config)# snmp-server community public ro
```

Use the following commands to remove an SNMP community called 'public'

```
awplus# configure terminal
awplus(config)# no snmp-server community public
```

Related commands

show snmp-server

show snmp-server community

snmp-server view

snmp-server contact

Overview This command sets the contact information for the system. The contact name is:

- displayed in the output of the show system command
- stored in the MIB object sysContact

The **no** variant of this command removes the contact information from the system.

Syntax

```
snmp-server contact <contact-info>
no snmp-server contact
```

Parameter	Description
<contact-info>	The contact information for the system, from 0 to 255 characters long. Valid characters are any printable character and spaces.

Mode Global Configuration

Example To set the system contact information to "support@alliedtelesis.co.nz", use the command:

```
awplus# configure terminal
awplus(config)# snmp-server contact
support@alliedtelesis.co.nz
```

Related commands

show system

snmp-server location

snmp-server group

snmp-server enable trap

Overview Use this command to enable the transmission of the specified notifications (traps) on your device.

Note that the Environmental Monitoring traps defined in the AT-ENVMONv2-MIB are enabled by default.

Use the **no** variant of this command to disable the transmission of the specified notifications.

Syntax

```
snmp-server enable trap <trap-list>
no snmp-server enable trap <trap-list>
```

Depending on your device model, you can enable some or all of the traps in the following table:

Parameter	Description
`atmf`	AMF traps.
`atmfguestnode`	AMF guest node traps.
`atmflink`	AMF link traps.
`atmfnode`	AMF node traps.
`atmfrr`	AMF reboot-rolling traps.
`auth`	Authentication failure.
`bgp`	BGP traps.
`chassis`	Chassis traps.
`cwmap`	Access Point traps with the AWC wireless manager.
`dhcpsnooping`	DHCP snooping and ARP security traps. These notifications must also be set using the **ip dhcp snooping violation** command, and/or the **arp security violation** command.
`epsr`	EPSR traps.
`g8032`	G.8032 ERP traps.
`lldp`	Link Layer Discovery Protocol (LLDP) traps. These notifications must also be enabled using the **lldp notifications** command, and/or the **lldp med-notifications** command.
`loopprot`	Loop Protection traps.

Parameter	Description
`low-memory`	Traps that are generated when available memory drops beneath low, very low, and critical thresholds, and when it returns to normal. The traps are: • 1.3.6.1.4.1.207.8.4.4.3.7.0 memoryTraps • 1.3.6.1.4.1.207.8.4.4.3.7.0.1 memoryLowTrap • 1.3.6.1.4.1.207.8.4.4.3.7.0.2 memoryVeryLowTrap • 1.3.6.1.4.1.207.8.4.4.3.7.0.3 memoryCriticalTrap (However, note that when the system reaches the critical memory threshold, it reboots before a trap can be sent.) • 1.3.6.1.4.1.207.8.4.4.3.7.0.4 memoryReturnToNormalTrap • 1.3.6.1.4.1.207.8.4.4.3.7.0.5 vcstackId
`mac-change`	MAC address changed.
`mac-move`	MAC address moved between interface.
`mac-threshold`	MAC address table reaches a threshold limit.
`mstp`	MSTP traps.
`nsm`	NSM traps.
`ospf`	OSPF traps.
`pim`	PIM traps.
`power-inline`	Power-inline traps (Power Ethernet MIB RFC 3621).
`qsp`	QoS Storm Protection.
`rmon`	RMON traps.
`thrash-limit`	MAC address Thrash Limiting traps.
`vcs`	VCS traps.
`vrrp`	Virtual Router Redundancy (VRRP) traps.
`ufo`	Upstream Forwarding Only (UFO) traps.

Default Disabled

Mode Global Configuration

Usage notes This command cannot be used to enable link status notifications globally. To enable link status notifications for particular interfaces, use the snmp trap link-status command.

To specify where notifications are sent, use the snmp-server host command.

Note that you can enable (or disable) multiple traps with a single command, by specifying a space-separated list of traps.

Examples

To enable the device to send a notification if an AMF node changes its status, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap atmfnode
```

Related commands

show snmp-server

snmp trap link-status

snmp-server host

Command changes

Version 5.5.4-2.3: **low-memory** parameter added

Version 5.5.1-2.1: **mac-change**, **mac-move**, and **mac-threshold** parameters added

Version 5.5.1-1.1: **atmfguestnode** and **cwmap** parameters added

Version 5.4.7-2.1: **ufo** parameter added

snmp-server engineID local

Overview Use this command to configure the SNMPv3 engine ID. The SNMPv3 engine ID is used to uniquely identify the SNMPv3 agent on a device when communicating with SNMP management clients. Once an SNMPv3 engine ID is assigned, this engine ID is permanently associated with the device until you change it.

Use the **no** variant of this command to set the user defined SNMPv3 engine ID to a system generated pseudo-random value by resetting the SNMPv3 engine. The **no snmp-server engineID local** command has the same effect as the **snmp-server engineID local default** command.

Note that the snmp-server engineID local reset command is used to force the system to generate a new engine ID when the current engine ID is also system generated.

Syntax

```
snmp-server engineID local {<engine-id>|default}
no snmp-server engineID local
```

Parameter	Description
<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 snmp-server engineID local reset command to force the system to generate a new engine ID.

Mode Global Configuration

Usage notes All devices must have a unique engine ID which is permanently set unless it is configured by the user.

Example To set the SNMPv3 engine ID to 800000cf030000cd123456, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local
800000cf030000cd123456
```

To set a user defined SNMPv3 engine ID back to a system generated value, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server engineID local
```

Output The following example shows the engine ID values after configuration:

```
awplus(config)#snmp-server engineid local asdgdfh231234d
awplus(config)#exit
awplus#show snmp-server

SNMP Server ........................... Enabled
IP Protocol ........................... IPv4
SNMPv3 Engine ID (configured name) ... asdgdfh231234d
SNMPv3 Engine ID (actual) ............ 0x80001f888029af52e149198483

awplus(config)#no snmp-server engineid local
awplus(config)#exit
awplus#show snmp-server

SNMP Server ........................... Enabled
IP Protocol ........................... IPv4
SNMPv3 Engine ID (configured name) ... Not set
SNMPv3 Engine ID (actual) ............ 0x80001f888029af52e149198483
```

Related commands

show snmp-server

snmp-server engineID local reset

snmp-server group

snmp-server engineID local reset

Overview Use this command to force the device to generate a new pseudo-random SNMPv3 engine ID by resetting the SNMPv3 engine. If the current engine ID is user defined, use the snmp-server engineID local command to set SNMPv3 engine ID to a system generated value.

Syntax

```
snmp-server engineID local reset
```

Mode Global Configuration

Example To force the SNMPv3 engine ID to be reset to a system generated value, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local reset
```

Related commands snmp-server engineID local

show snmp-server

snmp-server group

Overview This command is used with SNMP version 3 only, and adds an SNMP group, optionally setting the security level and view access modes for the group. The security and access views defined for the group represent the minimum required of its users in order to gain access.

The **no** variant of this command deletes an SNMP group, and is used with SNMPv3 only. The group with the specified authentication/encryption parameters must already exist.

Syntax

```
snmp-server group <groupname> {auth|noauth|priv} [read
<readname>|write <writename>|notify <notifyname>]
```

```
no snmp-server group <groupname>
```

Parameter	Description
<groupname>	Group name. The group name is a string up to 20 characters long and is case sensitive.
`auth`	Authentication.
`noauth`	No authentication and no encryption.
`priv`	Authentication and encryption.
`read`	Configure read view.
<readname>	Read view name.
`write`	Configure write view.
<writename>	Write view name. The view name is a string up to 20 characters long and is case sensitive.
`notify`	Configure notify view.
<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, user the following commands:

```
awplus# configure terminal
```

```
awplus(config)# snmp-server group usergroup noauth read
useraccess write useraccess
```

To delete the SNMP group called 'usergroup', use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# no snmp-server group usergroup
```

Related commands

snmp-server

show snmp-server

show snmp-server group

show snmp-server user

snmp-server host

Overview This command specifies an SNMP trap host destination to which Trap or Inform messages generated by the device are sent.

For SNMP version 1 and 2c you must specify the community name parameter. For SNMP version 3, specify the authentication/encryption parameters and the user name. If the version is not specified, the default is SNMP version 1. Inform messages can be sent instead of traps for SNMP version 2c and 3.

Use the **no** variant of this command to remove an SNMP trap host. The trap host must already exist.

The trap host is uniquely identified by:

- host IP address (IPv4 or IPv6)
- inform or trap messages
- community name (SNMPv1 or SNMP v2c) or the authentication/encryption parameters and user name (SNMP v3).

Syntax

```
snmp-server host {<ipv4-address>|<ipv6-address>} [traps]
[version 1] <community-name>

snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 2c <community-name>

snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 3 {auth|noauth|priv} <user-name>

no snmp-server host {<ipv4-address>|<ipv6-address>} [traps]
[version 1] <community-name>

no snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 2c <community-name>

no snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 3 {auth|noauth|priv} <user-name>
```

Parameter	Description
<ipv4-address>	IPv4 trap host address in the format A.B.C.D, for example, 192.0.2.2.
<ipv6-address>	IPv6 trap host address in the format x:x::x:x for example, 2001:db8::8a2e:7334.
`informs`	Send Inform messages to this host.
`traps`	Send Trap messages to this host (default).
`version`	SNMP version to use for notification messages. Default: version 1.
`1`	Use SNMPv1 (default).
`2c`	Use SNMPv2c.
`3`	Use SNMPv3.

Parameter	Description
`auth`	Authentication.
`noauth`	No authentication.
`priv`	Encryption.
<community-name>	The SNMPv1 or SNMPv2c community name.
<user-name>	SNMPv3 user name.

Default No host is defined.

Mode Global Configuration

Examples To configure the device to send generated traps to the IPv4 host destination 192.0.2.5 with the SNMPv2c community name 'public', use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server host 192.0.2.5 version 2c public
```

To configure the device to send generated traps to the IPv6 host destination 2001:db8::8a2e:7334 with the SNMPv2c community name 'private', use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server host 2001:db8::8a2e:7334 version 2c
private
```

To remove a configured trap host of 192.0.2.5 with the SNMPv2c community name 'public', use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server host 192.0.2.5 version 2c public
```

Related commands snmp trap link-status

snmp-server enable trap

snmp-server view

Command changes Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

snmp-server legacy-ifadminstatus

Overview Use this command to set the ifAdminStatus to reflect the operational state of the interface, rather than the administrative state.

The **no** variant of this command sets the ifAdminStatus to reflect the administrative state of the interface.

Syntax

```
snmp-server legacy-ifadminstatus
no snmp-server legacy-ifadminstatus
```

Default Legacy ifAdminStatus is turned off by default, so by default the SNMP ifAdminStatus reflects the administrative state of the interface.

Mode Global Configuration

Usage notes Note that if you enable Legacy ifAdminStatus, the ifAdminStatus will report a link's status as Down when the link has been blocked by a process such as loop protection.

Example To turn on Legacy ifAdminStatus, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server legacy-ifadminstatus
```

Related commands show interface

snmp-server location

Overview This command sets the location of the system. The location is:

- displayed in the output of the show system command
- stored in the MIB object sysLocation

The **no** variant of this command removes the configured location from the system.

Syntax

```
snmp-server location <location-name>
no snmp-server location
```

Parameter	Description
<location-name>	The location of the system, from 0 to 255 characters long. Valid characters are any printable character and spaces.

Mode Global Configuration

Example To set the location to “server room 523”, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server location server room 523
```

Related commands

show snmp-server

show system

snmp-server contact

snmp-server source-interface

Overview Use this command to specify the originating interface for SNMP traps or informs. An interface specified by this command must already have an IP address assigned to it.

Use the **no** variant of this command to reset the interface to its default value (the originating egress interface).

Syntax

```
snmp-server source-interface {traps|informs} <interface-name>
no snmp-server source-interface {traps|informs}
```

Parameter	Description
`traps`	SNMP traps.
`informs`	SNMP informs.
<interface-name>	Interface name (must already have an IP address assigned).

Default The originating egress interface of the traps and informs messages

Mode Global Configuration

Usage notes When an SNMP server sends an SNMP trap or inform message, the message carries the notification IP address of its originating interface. Use this command to assign this interface.

Example The following commands set eth0 to be the interface whose IP address is used as the originating address in SNMP informs packets.

```
awplus# configure terminal
awplus(config)# snmp-server source-interface informs eth0
```

The following commands reset the originating source interface for SNMP trap messages to be the default interface (the originating egress interface):

```
awplus# configure terminal
awplus(config)# no snmp-server source-interface traps
```

Validation Commands show running-config

snmp-server startup-trap-delay

Overview Use this command to set the time in seconds after following completion of the device startup sequence before the device sends any SNMP traps (or SNMP notifications).

Use the no variant of this command to restore the default startup delay of 30 seconds.

Syntax

```
snmp-server startup-trap-delay <delay-time>
no snmp-server startup-trap-delay
```

Parameter	Description
<delay-time>	Specify an SNMP trap delay time in seconds in the range of 30 to 600 seconds.

Default The SNMP server trap delay time is 30 seconds. The no variant restores the default.

Mode Global Configuration

Example To delay the device sending SNMP traps until 60 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server startup-trap-delay 60
```

To restore the sending of SNMP traps to the default of 30 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server startup-trap-delay
```

Validation Commands show snmp-server

snmp-server user

Overview Use this command to create or move users as members of specified groups. This command is used with SNMPv3 only.

The **no** variant of this command removes an SNMPv3 user. The specified user must already exist.

Syntax

```
snmp-server user <username> <groupname> [encrypted] [auth
{md5|sha} <auth-password>] [priv {des|aes} <privacy-password>]
```

```
no snmp-server user <username>
```

Parameter	Description
<username>	User name. The user name is a string up to 20 characters long and is case sensitive.
<groupname>	Group name. The group name is a string up to 20 characters long and is case sensitive.
`encrypted`	Use the encrypted parameter when you want to enter encrypted passwords.
`auth`	Authentication protocol.
`md5`	MD5 Message Digest Algorithms.
`sha`	SHA Secure Hash Algorithm.
<auth-password>	Authentication password. The password is a string of 8 to 20 characters long and is case sensitive.
`priv`	Privacy protocol.
`des`	DES: Data Encryption Standard.
`aes`	AES: Advanced Encryption Standards.
<privacy-password>	Privacy password. The password is a string of 8 to 20 characters long and is case sensitive.

Mode Global Configuration

Usage notes Additionally this command provides the option of selecting an authentication protocol and (where appropriate) an associated password. Similarly, options are offered for selecting a privacy protocol and password.

- Note that each SNMP user must be configured on both the manager and agent entities. Where passwords are used, these passwords must be the same for both entities.
- Use the **encrypted** parameter when you want to enter already encrypted passwords in encrypted form as displayed in the running and startup configs stored on the device. For example, you may need to move a user from one group to another group and keep the same passwords for the user instead of removing the user to apply new passwords.

- User passwords are entered using plaintext without the **encrypted** parameter and are encrypted according to the authentication and privacy protocols selected.
- User passwords are viewed as encrypted passwords in running and startup configs shown from **show running-config** and **show startup-config** commands respectively. Copy and paste encrypted passwords from running-configs or startup-configs to avoid entry errors.

Examples To add SNMP user authuser as a member of group 'usergroup', with authentication protocol MD5, authentication password 'Authpass', privacy protocol AES and privacy password 'Privpass' use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server user authuser usergroup auth md5
Authpass priv aes Privpass
```

Validate the user is assigned to the group using the **show snmp-server user** command:

```
awplus#show snmp-server user
Name                Group name          Auth         Privacy
-------             -------------       -------      ----------
authuser            usergroup           md5          aes
```

To enter existing SNMP user 'authuser' with existing passwords as a member of group 'newusergroup' with authentication protocol MD5 with the encrypted authentication password 0x1c74b9c22118291b0ce0cd883f8dab6b74, and privacy protocol AES with the encrypted privacy password 0x0e0133db5453ebd03822b004eeacb6608f, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server user authuser newusergroup
encrypted auth md5 0x1c74b9c22118291b0ce0cd883f8dab6b74 priv
aes 0x0e0133db5453ebd03822b004eeacb6608f
```

NOTE: *Copy and paste the encrypted passwords from the **running-config** or the **startup-config** displayed, using the **show running-config** and **show startup- config** commands respectively, into the command line to avoid key stroke errors issuing this command.*

Validate the user has been moved from the first group using the **show snmp-server user** command:

```
awplus#show snmp-server user
Name                Group name          Auth         Privacy
-------             -------------       -------      ----------
authuser            newusergroup        md5          aes
```

To delete SNMP user 'authuser', use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server user authuser
```

Related commands

show snmp-server user

snmp-server view

snmp-server view

Overview Use this command to create an SNMP view that specifies a sub-tree of the MIB. Further sub-trees can then be added by specifying a new OID to an existing view. Views can be used in SNMP communities or groups to control the remote manager's access.

NOTE: *The object identifier must be specified in a sequence of integers separated by decimal points.*

The **no** variant of this command removes the specified view on the device. The view must already exist.

Syntax

```
snmp-server view <view-name> <mib-name> {included|excluded}
no snmp-server view <view-name>
```

Parameter	Description
`<view-name>`	SNMP server view name. 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

undebug snmp

Overview This command applies the functionality of the no debug snmp command.

28 Mail (SMTP) Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure mail. The mail feature uses Simple Mail Transfer Protocol (SMTP) to transfer mail from an internal email client operating within the AlliedWare Plus device. This feature is typically used to email event notifications to an external email server from the AlliedWare Plus device.

For information on using the mail feature, see the Mail (SMTP) Feature Overview and Configuration Guide.

Command List

- "debug mail" on page 937
- "delete mail" on page 938
- "mail" on page 939
- "mail from" on page 941
- "mail smtpserver" on page 942
- "mail smtpserver authentication" on page 943
- "mail smtpserver port" on page 945
- "mail smtpserver tls" on page 947
- "show counter mail" on page 948
- "show mail" on page 949
- "undebug mail" on page 950

debug mail

Overview This command turns on debugging for sending emails.

The **no** variant of this command turns off debugging for sending emails.

Syntax

```
debug mail
no debug mail
```

Mode Privileged Exec

Examples To turn on debugging for sending emails, use the command:

```
awplus# debug mail
```

To turn off debugging for sending emails, use the command:

```
awplus# no debug mail
```

Related commands

delete mail

mail

mail from

mail smtpserver

show counter mail

show mail

undebug mail

delete mail

Overview This command deletes mail from the queue.

You need the *mail-id* from the **show mail** command output to delete specific emails, or use the **all** parameter to clear all messages in the queue completely.

Syntax

```
delete mail [mail-id <mail-id>|all]
```

Parameter	Description	
`mail-id`	Deletes a single mail from the mail queue.	
	<mail-id>	A unique mail ID number. Use the show mail command to display this for an item of mail.
`all`	Delete all the mail in the queue.	

Mode Privileged Exec

Examples To delete the unique mail item "20060912142356.1234" from the queue, use the command:

```
awplus# delete mail 20060912142356.1234
```

To delete all mail from the queue, use the command:

```
awplus# delete mail all
```

Related commands

debug mail

mail

mail from

mail smtpserver

show mail

mail

Overview This command sends an email using the SMTP protocol. If you specify a file the text inside the file is sent in the message body.

If you do not specify the **to**, **file**, or **subject** parameters, the CLI prompts you for the missing information.

Before you can send mail using this command, you must specify the sending email address using the mail from command and a mail server using the mail smtpserver command.

Syntax `mail [to <to>] [subject <subject>] [file <filename>]`

Parameter	Description	
`to`	The email recipient.	
	<to>	Email address.
`subject`	Description of the subject of this email. Use quote marks when the subject text contains spaces.	
	<subject>	String.
`file`	File to insert as text into the message body.	
	<filename>	String.

Mode Privileged Exec

Usage notes When you use the **mail** command you can use parameter substitutions in the subject field. The following table lists the parameters that can be substituted and their descriptions:

Parameter	Description
<%N>	When this parameter is specified, the %N is replaced by the host name of your device.
<%S>	When this parameter is specified, the %S is replaced by the serial number of your device.
<%D> *<%L>* *<%T>*	When any of these parameters is specified, they are replaced by the current date and time (local time) on your device.
<%U>	When this parameter is specified, the %U is replaced by the current date and time (UTC time) on your device.

NOTE: *If no local time is configured, it will use UTC.*

Examples

To send an email to “admin@example.com” with the subject “test email” and with the message body inserted from the file “test.conf”, use the command:

```
awplus# mail to admin@example.com subject "test email" filename
test.conf
```

To send an email using parameter substitutions for the host name, serial number and date, use the commands:

```
awplus# mail to admin@example.com subject "Sending email from
Hostname:%N Serial Number:%S Date:%T"
```

Related commands

debug mail

delete mail

mail from

mail smtpserver

mail smtpserver authentication

mail smtpserver port

show counter mail

show mail

mail from

Overview This command sets an email address as the sender. You must specify a sending email address with this command before you can send email.

Use the **no** variant of this command to remove the "mail from" address.

Syntax

```
mail from <from>
no mail from
```

Parameter	Description
<from>	The email address that the mail is sent from (also known as the hostname).

Mode Global Configuration

Example To set up your email address as the sender "kaji@nerv.com", use the command:

```
awplus(config)# mail from kaji@nerv.com
```

Related commands

debug mail

delete mail

mail

mail smtpserver

show counter mail

show mail

undebug mail

mail smtpserver

Overview This command specifies the IP address or domain name of the SMTP server that your device sends email to. You must specify a mail server with this command before you can send email.

Use the **no** variant of this command to remove the configured mail server.

Syntax

```
mail smtpserver {<ip-address>|<name>}
no mail smtpserver
```

Parameter	Description
<ip-address>	Internet Protocol (IP) address for the mail server.
<name>	Domain name (FQDN) for the mail server (also known as the host name).

Mode Global Configuration

Usage notes If you specify the server by specifying its domain name, you must also ensure that the DNS client on your device is enabled. It is enabled by default but if it has been disabled, you can re-enable it by using the ip domain-lookup command.

Examples To specify a mail server at "192.168.0.1", use the command:

```
awplus(config)# mail smtpserver 192.168.0.1
```

To specify a mail server that has a host name of "smtp.example.com", use the command:

```
awplus(config)# mail smtpserver smtp.example.com
```

To remove the configured mail server, use the command:

```
awplus(config)# no mail smtpserver
```

Related commands

debug mail

delete mail

mail

mail from

show counter mail

show mail

mail smtpserver authentication

Overview Use this command to configure SMTP mail server authentication.

Use the **no** variant of this command to remove the configured SMTP mail server authentication.

Syntax

```
mail smtpserver authentication {crammd5|login|plain} username
<username> password [8] <password>
```

```
no mail smtpserver authentication
```

Parameter	Description
`crammd5`	This is a Challenge Request Authentication Mechanism based on the HMAC-MD5 mechanism and is the most secure option.
`login`	A BASE64 encryption method
`plain`	A BASE64 encryption method
<username>	Registered user name
`8`	The registered user password is presented in an already encrypted format. This is how the running configuration stores the plain text password and is not for general use.
<password>	Registered user password

Default No authentication option is set by default.

Mode Global Configuration

Usage notes You cannot change the IP address or Domain Name of the SMTP server if authentication is configured. If you attempt to change it when authentication is configured, the following error message is displayed:

```
% Error: authentication configuration still exists
```

Examples To configure the SMTP mail server authentication to crammd5, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# mail smtpserver authentication crammd5 username
admin password unguessablePassword
```

To remove SMTP mail server authentication, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no mail smtpserver authentication
```

Output Figure 28-1: Example output from **show mail**:

```
awplus#show mail
Mail Settings
-------------------------------------------------------------
State                                : Alive
SMTP Server                          : 1.2.3.4
Host Name                            : admin@example.com
Authentication                       : crammd5
Username                             : admin
Debug                                : Disabled

awplus#show running-config
!
mail smtpserver authentication plain username admin password 8
aF0a9pkjbmXGfl6TlSk/GakeIK5tMYN6LqMYT8Ia2qw=
!
```

Related commands

debug mail

delete mail

mail

mail from

mail smtpserver

mail smtpserver port

show counter mail

show mail

Command changes Version 5.4.8-1.1: command added

mail smtpserver port

Overview Use this command to configure the SMTP mail client/server communication port.

Use the **no** variant of this command to remove the configured port and set it back to the default port.

Syntax

```
mail smtpserver port <port>
no mail smtpserver port
```

Parameter	Description
<port>	Port number from the range 1 to 65535

Default The default port value is 25 if TLS is not enabled for the SMTP server, 587 if TLS is enabled with STARTTLS, and 465 if TLS is enabled with SMTPS.

Mode Global Configuration

Examples To configure the mail server communication over port 587, use the commands:

```
awplus# configure terminal
awplus(config)# mail smtpserver port 587
```

To revert to the default SMTP mail server communication port, use the commands:

```
awplus# configure terminal
awplus(config)# no mail smtpserver port
```

Output Figure 28-2: Example output from **show mail**:

```
awplus#show mail
Mail Settings
-------------------------------------------------------------
State                                : Alive
SMTP Server                          : 10.24.165.4
Host Name                            : admin@example.com
Authentication                       : plain
Username                             : admin
Port                                 : 587
Use TLS                              : STARTTLS
Debug                                : Disabled

awplus#show running-config
!
mail smtpserver port 587
!
```

Related commands debug mail

delete mail

mail

mail from

mail smtpserver

mail smtpserver tls

show counter mail

show mail

Command changes Version 5.4.8-1.1: command added

mail smtpserver tls

Overview Use this command to configure the device to send emails over a TLS connection to the SMTP server instead of sending in clear-text. If the SMTP server does not support receiving emails over a TLS connection, sending emails from the device will fail.

Use the **no** variant of this command to configure the device to send emails over an unencrypted TCP connection (clear text).

Syntax

```
mail smtpserver tls [starttls|smtps]
no mail smtpserver tls
```

Parameter	Description
`starttls`	The connection starts as clear-text SMTP first and then the client establishes a TLS connection using the STARTTLS extension.
`smtps`	Use a TLS connection from the start.

Default By default, TLS is disabled and the device sends emails in clear-text.

Mode Global Configuration

Examples To send emails to the SMTP server over a TLS connection that will be established by the STARTTLS method, use the commands:

```
awplus# configure terminal
awplus(config)# mail smtpserver tls starttls
```

To send emails to the SMTP server over a TLS connection from the beginning, use the commands:

```
awplus# configure terminal
awplus(config)# mail smtpserver tls smpts
```

To send emails to the SMTP server in clear text, use the commands:

```
awplus# configure terminal
awplus(config)# no mail smtpserver tls
```

Related commands

mail

show mail

mail smtpserver

mail smtpserver port

mail smtpserver authentication

Command changes Version 5.5.3-0.1: command added

show counter mail

Overview This command displays the mail counters.

Syntax

```
show counter mail
```

Mode User Exec and Privileged Exec

Example To show the emails in the queue use the command:

```
awplus# show counter mail
```

Output Figure 28-3: Example output from the **show counter mail** command

```
Mail Client (SMTP) counters
Mails Sent            ......... 2
Mails Sent Fails      ......... 1
```

Table 1: Parameters in the output of the **show counter mail** command

Parameter	Description
`Mails Sent`	The number of emails sent successfully since the last device restart.
`Mails Sent Fails`	The number of emails the device failed to send since the last device restart.

Related commands

debug mail

delete mail

mail

mail from

show mail

show mail

Overview This command displays the emails in the queue.

Syntax

```
show mail
```

Mode Privileged Exec

Example To display the emails in the queue use the command:

```
awplus# show mail
```

Output Figure 28-4: Example output from the **show mail** command:

```
awplus#show mail
Mail Settings
-------------------------------------------------------------
State                               : Alive
SMTP Server                         : example.net
Host Name                           : test@example.com
Authentication                      : login
Username                            : admin
Port                                : 587
Use TLS                             : STARTTLS
Debug                               : Disabled

Messages
-------------------------------------------------------------
There is no mail in the queue.
```

Related commands

delete mail

mail

mail from

mail smtpserver

mail smtpserver tls

show counter mail

mail smtpserver port

undebug mail

undebug mail

Overview This command applies the functionality of the no debug mail command.

29 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 953
- "clear ssh" on page 954
- "crypto key destroy hostkey" on page 955
- "crypto key destroy userkey" on page 956
- "crypto key generate hostkey" on page 957
- "crypto key generate userkey" on page 959
- "crypto key pubkey-chain knownhosts" on page 961
- "crypto key pubkey-chain userkey" on page 963
- "debug ssh client" on page 965
- "debug ssh server" on page 966
- "service ssh" on page 967
- "show banner login" on page 969
- "show crypto key hostkey" on page 970
- "show crypto key pubkey-chain knownhosts" on page 972
- "show crypto key pubkey-chain userkey" on page 974
- "show crypto key userkey" on page 975
- "show running-config ssh" on page 976
- "show ssh" on page 978
- "show ssh client" on page 980

- "show ssh server" on page 981
- "show ssh server allow-users" on page 983
- "show ssh server deny-users" on page 984
- "ssh" on page 985
- "ssh client" on page 987
- "ssh client allow-legacy-ssh-rsa" on page 989
- "ssh server" on page 990
- "ssh server allow-legacy-ssh-rsa" on page 992
- "ssh server allow-users" on page 993
- "ssh server authentication" on page 995
- "ssh server deny-users" on page 997
- "ssh server max-auth-tries" on page 999
- "ssh server resolve-host" on page 1000
- "ssh server scp" on page 1001
- "ssh server secure-algs" on page 1002
- "ssh server secure-ciphers" on page 1003
- "ssh server secure-hostkey" on page 1004
- "ssh server secure-kex" on page 1005
- "ssh server secure-mac" on page 1006
- "ssh server sftp" on page 1007
- "ssh server tcpforwarding" on page 1008
- "undebug ssh client" on page 1009
- "undebug ssh server" on page 1010

banner login (SSH)

Overview This command configures a login banner on the SSH server. This displays a message on the remote terminal of the SSH client before the login prompt. SSH client version 1 does not support this banner.

To add a banner, first enter the command **banner login**, and hit [Enter]. Write your message. You can use any character and spaces. Use Ctrl+D at the end of your message to save the text and re-enter the normal command line mode.

The banner message is preserved if the device restarts.

The **no** variant of this command deletes the login banner from the device.

Syntax

```
banner login
no banner login
```

Default No banner is defined by default.

Mode Global Configuration

Examples To set a login banner message, use the commands:

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

The screen will prompt you to enter the message:

```
Type CNTL/D to finish.
... banner message comes here ...
```

Enter the message. Use Ctrl+D to finish, like this:

```
^D
awplus(config)#
```

To remove the login banner message, use the commands:

```
awplus# configure terminal
awplus(config)# no banner login
```

Related commands show banner login

clear ssh

Overview This command deletes Secure Shell sessions currently active on the device. This includes both incoming and outgoing sessions. The deleted sessions are closed. You can only delete an SSH session if you are a system manager or the user who initiated the session. If **all** is specified then all active SSH sessions are deleted.

Syntax

```
clear ssh {<1-65535>|all}
```

Parameters	Description
<1-65535>	Specify a session ID in the range 1 to 65535 to delete a specific session.
`all`	Delete all SSH sessions.

Mode Privileged Exec

Examples To stop the current SSH session 123, use the command:

```
awplus# clear ssh 123
```

To stop all SSH sessions active on the device, use the command:

```
awplus# clear ssh all
```

Related commands service ssh

ssh

crypto key destroy hostkey

Overview This command deletes the existing public and private keys of the SSH server.

Syntax

```
crypto key destroy hostkey {dsa|ecdsa|ed25519|rsa|rsa1}
```

Parameters	Description
`dsa`	Deletes the existing DSA public and private keys.
`ecdsa`	Deletes the existing ECDSA public and private keys.
`ed25519`	Deletes the existing Ed25519 public and private keys.
`rsa`	Deletes the existing RSA public and private keys that were configured for SSH version 2 connections.
`rsa1`	Deletes the existing RSA public and private keys that were configured for SSH version 1 connections. From AlliedWare Plus version 5.5.1-1.1 onwards, SSH version 1 is not supported.

Mode Global Configuration

Example To destroy the RSA host key used for SSH version 2 connections, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy hostkey rsa
```

Related commands crypto key generate hostkey

service ssh

Command changes Version 5.5.2-2.1: **ed25519** parameter added

crypto key destroy userkey

Overview This command destroys the existing public and private keys of an SSH user configured on the device.

Syntax
```
crypto key destroy userkey <username>
{dsa|ecdsa|ed25519|rsa|rsa1}
```

Parameters	Description
<*username*>	Name of the user whose userkey you are destroying. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
dsa	Deletes the existing DSA userkey.
ecdsa	Deletes the existing ECDSA userkey.
ed25519	Deletes the existing Ed25519 userkey.
rsa	Deletes the existing RSA userkey that was configured for SSH version 2 connections.
rsa1	Deletes the existing RSA userkey that was configured for SSH version 1 connections. From AlliedWare Plus version 5.5.1-1.1 onwards, SSH version 1 is not supported.

Mode Global Configuration

Example To destroy the RSA user key for the SSH user `remoteuser`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy userkey remoteuser rsa
```

Related commands

crypto key generate hostkey

crypto key generate userkey

show ssh

show crypto key hostkey

Command changes Version 5.5.2-2.1: **ed25519** parameter added

crypto key generate hostkey

Overview This command generates public and private keys for the SSH server.

When you enable the SSH server, if no host keys exist, the server automatically generates SSHv2 host key pairs using Ed25519 with a keysize of 256, ECDSA with a curve length of 384, and RSA with a 2048-bit key.

If you need a key with different parameters than this, you can use this command to generate that key before you enable the SSH server. If a host key exists with the same cryptography algorithm, this command replaces the old host key with the new key.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

Syntax

```
crypto key generate hostkey rsa [<1024-16384>]
crypto key generate hostkey ecdsa [<256|384|521>]
crypto key generate hostkey ed25519
```

Parameters	Description
rsa	Creates an RSA hostkey.
ecdsa	Creates an ECDSA hostkey.
ed25519	Creates an Ed25519 hostkey with a keysize of 256.
<1024-16384>	The length in bits of the generated key.
<256|384|521>	The ECDSA key size in bits.

Default The default key length for RSA is 2048 bits.

The default key size for ECDSA is 384 bits.

Mode Global Configuration

Examples To generate an RSA host key that is 4096 bits in length, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 4096
```

To generate an ECDSA host key with an elliptic curve size of 521 bits, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey ecdsa 521
```

To generate an Ed25519 host key with a keysize of 256, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey ed25519
```

Related commands

crypto key destroy hostkey

service ssh

show crypto key hostkey

Command changes

Version 5.5.2-2.1: **ed25519** parameter added

Version 5.5.2-0.1: changes to key length and key size ranges and defaults

Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

crypto key generate userkey

Overview This command generates public and private keys for an SSH user using an RSA, ECDSA, or ED25519 cryptography algorithm. To use public key authentication, copy the public key of the user onto the remote SSH server.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

Syntax

```
crypto key generate userkey <username> rsa [<1024-16384>]
crypto key generate userkey <username> ecdsa [<256|384|521>]
crypto key generate userkey <username> ed25519
```

Parameters	Description
<username>	Name of the user that the user key is generated for. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
rsa	Creates an RSA userkey.
ecdsa	Creates an ECDSA userkey.
ed25519	Creates an Ed25519 userkey with a keysize of 256.
<1024-16384>	The length in bits of the generated key. The default is 2048 bits.
<256|384|521>	The ECDSA key size in bits. The default is 384.

Default The default key length for RSA is 2048 bits.

The default key size for ECDSA is 384 bits.

Mode Global Configuration

Examples To generate a 4096-bit RSA user key for SSH version 2 connections for the user 'bob', use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey bob rsa 4096
```

To generate an ECDSA user key of key size 521 for the user 'lapo', use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo ecdsa 521
```

To generate an Ed25519 user key of key size 256 for the user 'lapo', use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo ed25519
```

Related commands

crypto key pubkey-chain userkey

show crypto key userkey

Command changes

Version 5.5.2-2.1: **ed25519** parameter added

Version 5.5.2-0.1: changes to key length and key size ranges and defaults

Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

crypto key pubkey-chain knownhosts

Overview This command adds a public key of the specified SSH server to the known host database on your device. The SSH client on your device uses this public key to verify the remote SSH server.

The key is retrieved from the server. Before adding a key to this database, check that the key sent to you is correct.

If the server's key changes, or if your SSH client does not have the public key of the remote SSH server, then your SSH client will inform you that the public key of the server is unknown or altered.

The **no** variant of this command deletes the public key of the specified SSH server from the known host database on your device.

Syntax

```
crypto key pubkey-chain knownhosts [ip|ipv6] <hostname>
[ecdsa|rsa]
no crypto key pubkey-chain knownhosts <1-65535>
```

Parameter	Description
`ip`	Keyword used prior to specifying an IPv4 address
`ipv6`	Keyword used prior to specifying an IPv6 address
<hostname>	IPv4/IPv6 address or hostname of a remote server in the format `a.b.c.d` for an IPv4 address, or in the format `x:x::x:x` for an IPv6 address.
`ecdsa`	Specify the ECDSA public key of the server to be added to the known host database.
`rsa`	Specify the RSA public key of the server to be added to the known host database.
<1-65535>	Specify a key identifier when removing a key using the **no** parameter.

Default If no cryptography algorithm is specified, then **rsa** is used as the default cryptography algorithm.

Mode Privilege Exec

Usage notes This command adds a public key of the specified SSH server to the known host database on the device. The key is retrieved from the server. The remote SSH server is verified by using this public key. The user is requested to check the key is correct before adding it to the database.

If the remote server's host key is changed, or if the device does not have the public key of the remote server, then SSH clients will inform the user that the public key of the server is altered or unknown.

Examples

To add the RSA host key of the remote SSH host IPv4 address 192.0.2.11 to the known host database, use the command:

```
awplus# crypto key pubkey-chain knownhosts 192.0.2.11
```

To delete the second entry in the known host database, use the command:

```
awplus# no crypto key pubkey-chain knownhosts 2
```

Validation Commands

show crypto key pubkey-chain knownhosts

crypto key pubkey-chain userkey

Overview This command adds a public key for an SSH user on the SSH server. This allows the SSH server to support public key authentication for the SSH user. When configured, the SSH user can access the SSH server without providing a password from the remote host.

The **no** variant of this command removes a public key for the specified SSH user that has been added to the public key chain. When a SSH user's public key is removed, the SSH user can no longer login using public key authentication.

Syntax

```
crypto key pubkey-chain userkey <username> [<filename>]
no crypto key pubkey-chain userkey <username> <1-65535>
```

Parameters	Description
<username>	Name of the user that the SSH server associates the key with. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. Default: no default
<filename>	Filename of a key saved in flash. Valid characters are any printable character. You can add a key as a hexadecimal string directly into the terminal if you do not specify a filename.
<1-65535>	The key ID number of the user's key. Specify the key ID to delete a key.

Mode Global Configuration

Usage notes You should import the public key file from the client node. The device can read the data from a file on the flash or user terminal.

Or you can add a key as text into the terminal. To add a key as text into the terminal, first enter the command **crypto key pubkey-chain userkey** <*username*>, and hit [Enter]. Enter the key as text. Note that the key you enter as text must be a valid SSH RSA key, not random ASCII text. Use [Ctrl]+D after entering it to save the text and re-enter the normal command line mode.

Note you can generate a valid SSH RSA key on the device first using the **crypto key generate host rsa** command. View the SSH RSA key generated on the device using the **show crypto hostkey rsa** command. Copy and paste the displayed SSH RSA key after entering the **crypto key pubkey-chain userkey** <*username*> command. Use [Ctrl]+D after entering it to save it.

Examples To generate a valid SSH RSA key on the device and add the key, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto key generate host rsa
awplus(config)# exit
awplus# show crypto key hostkey
rsaAAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fcOw1TStpb9J20bWluh
nUC768EoWhyPW6FZ2t5360O5M29EpKBmGqlkQaz5V0mU9IQe66+5YyD4UxOKSD
tTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/pqGDijj4SvfZZfe
ITzvvyZW4/I4pbN8=
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey joeType CNTL/D
to
finish:AAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fcOw1TStpb9J20b
WluhnUC768EoWhyPW6FZ2t5360O5M29EpKBmGqlkQaz5V0mU9IQe66+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

Command changes Version 5.5.3-1.1: added to AR1050V

debug ssh server

Overview This command enables the SSH server debugging facility. When enabled, the SSH server sends diagnostic messages to the system log. To display the debugging messages on the terminal, use the **terminal monitor** command.

The **no** variant of this command disables the SSH server debugging facility. This stops the SSH server from generating diagnostic debugging messages.

Syntax

```
debug ssh server [brief|full]
no debug ssh server
```

Parameter	Description
`brief`	Enables brief debug mode.
`full`	Enables full debug mode.

Default SSH server debugging is disabled by default.

Mode Privileged Exec and Global Configuration

Examples To start SSH server debugging, use the command:

```
awplus# debug ssh server
```

To start SSH server debugging with extended output, use the command:

```
awplus# debug ssh server full
```

To disable SSH server debugging, use the command:

```
awplus# no debug ssh server
```

Related commands

debug ssh client

show ssh server

undebug ssh server

service ssh

Overview Use this command to enable the Secure Shell server on the device. Once enabled, connections coming from SSH clients are accepted.

When you enable the SSH server, if no host keys exist, the server automatically generates SSHv2 host key pairs using ECDSA with a curve length of 384, and RSA with a 1024-bit key.

If you need a key with different parameters than this, you can use the crypto key generate hostkey command to generate that key before you enable the SSH server.

Use the **no** variant of this command to disable the Secure Shell server. When the Secure Shell server is disabled, connections from SSH, SCP, and SFTP clients are not accepted. This command does not affect existing SSH sessions. To terminate existing sessions, use the clear ssh command.

Syntax

```
service ssh [ip|ipv6]
no service ssh [ip|ipv6]
```

Default The Secure Shell server is disabled by default. Both IPv4 and IPv6 Secure Shell server are enabled when you issue **service ssh** without specifying the optional **ip** or **ipv6** parameters.

Mode Global Configuration

Examples To enable both the IPv4 and the IPv6 Secure Shell server, use the commands:

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

To enable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ip
```

To enable the IPv6 Secure Shell server only, use the commands:

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

To disable both the IPv4 and the IPv6 Secure Shell server, use the commands:

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

To disable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ip
```

To disable the IPv6 Secure Shell server only, use the commands:

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

Related commands

crypto key generate hostkey

show running-config ssh

show ssh server

ssh server allow-users

ssh server deny-users

Command changes

Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

show banner login

Overview This command displays the banner message configured on the device. The banner message is displayed to the remote user before user authentication starts.

Syntax

```
show banner login
```

Mode User Exec, Privileged Exec, Global Configuration, Interface Configuration, Line Configuration

Example To display the current login banner message, use the command:

```
awplus# show banner login
```

Related commands banner login (SSH)

show crypto key hostkey

Overview This command displays the public keys generated on the device for the SSH server.

When you enable the SSH server, if no host keys exist, the server automatically generates SSHv2 host key pairs using ECDSA with a curve length of 384, and RSA with a 1024-bit key.

The private key remains on the device secretly. The public key is copied to SSH clients to identify the server. This command displays the public key.

Syntax

```
show crypto key hostkey [dsa|ecdsa|rsa|rsa1]
```

Parameter	Description
dsa	Displays the DSA algorithm public key.
ecdsa	Displays the ECDSA algorithm public key.
rsa	Displays the RSA algorithm public key for SSH version 2 connections.
rsa1	Displays the RSA algorithm public key for SSH version 1 connections. From AlliedWare Plus 5.5.1-1.1 onwards, SSH version 1 is not supported.

Mode User Exec, Privileged Exec and Global Configuration

Examples To show the public keys generated on the device for SSH server, use the command:

```
awplus# show crypto key hostkey
```

To display the RSA public key of the SSH server, use the command:

```
awplus# show crypto key hostkey rsa
```

Output Figure 29-1: Example output from the **show crypto key hostkey** command

```
Type  Bits   Fingerprint
-------------------------------------------------------------
rsa   1024 SHA256:T/sVz5OoA1HHXcov9dXzGGQg8avRUYh1psxNSUcSOvs
ecdsa 384 SHA256:qVn/KpN5X5ct5CJakxE4OmPWmPvW2vIbBjF4SA2bZkM
```

Table 1: Parameters in output of the **show crypto key hostkey** command

Parameter	Description
Type	Algorithm used to generate the key.
Bits	Length in bits of the key.
Fingerprint	Checksum value for the public key.

Related commands

crypto key destroy hostkey

crypto key generate hostkey

show crypto key pubkey-chain knownhosts

Overview This command displays the list of public keys maintained in the known host database on the device.

Syntax
```
show crypto key pubkey-chain knownhosts [<1-65535>]
```

Parameter	Description
<1-65535>	Key identifier for a specific key. Displays the public key of the entry if specified.

Default Display all keys.

Mode User Exec, Privileged Exec and Global Configuration

Examples To display public keys of known SSH servers, use the command:

```
awplus# show crypto key pubkey-chain knownhosts
```

To display the key data of the first entry in the known host data, use the command:

```
awplus# show crypto key pubkey-chain knownhosts 1
```

Output Figure 29-2: 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:bcdf:ffff:0001
                       rsa1 af:4e:b4:a2:26:24:6d:65:20:32:d9:6f:32:06:ba:57
```

Table 2: Parameters in the output of the **show crypto key public-chain knownhosts** command

Parameter	Description
`No`	Number ID of the key.
`Hostname`	Host name of the known SSH server.
`Type`	The algorithm used to generate the key.
`Fingerprint`	Checksum value for the public key.

Related commands crypto key pubkey-chain knownhosts

Command changes

Version 5.5.3-1.1: added to AR1050V

Version 5.4.6-2.1: VRF-lite support added for AR-Series devices

show crypto key pubkey-chain userkey

Overview This command displays the public keys registered with the SSH server for SSH users. These keys allow remote users to access the device using public key authentication. By using public key authentication, users can access the SSH server without providing password.

Syntax

```
show crypto key pubkey-chain userkey <username> [<1-65535>]
```

Parameter	Description
<username>	User name of the remote SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
<1-65535>	Key identifier for a specific key.

Default Display all keys.

Mode User Exec, Privileged Exec and Global Configuration

Example To display the public keys for the user `manager` that are registered with the SSH server, use the command:

```
awplus# show crypto key pubkey-chain userkey manager
```

Output Figure 29-3: Example output from the **show crypto key public-chain userkey** command

```
No Type Bits Fingerprint
-------------------------------------------------------------------
1  dsa  1024 2b:cc:df:a8:f8:2e:8f:a4:a5:4f:32:ea:67:29:78:fd
2  rsa  2048 6a:ba:22:84:c1:26:42:57:2c:d7:85:c8:06:32:49:0e
```

Table 3: Parameters in the output of the **show crypto key userkey** command

Parameter	Description
`No`	Number ID of the key.
`Type`	The algorithm used to generate the key.
`Bits`	Length in bits of the key.
`Fingerprint`	Checksum value for the key.

Related commands crypto key pubkey-chain userkey

show crypto key userkey

Overview This command displays the public keys created on this device for the specified SSH user.

Syntax

```
show crypto key userkey <username> [dsa|rsa|rsa1]
```

Parameter	Description
<username>	User name of the local SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
dsa	Displays the DSA public key.
rsa	Displays the RSA public key used for SSH version 2 connections.
rsa1	Displays the RSA key used for SSH version 1 connections.

Mode User Exec, Privileged Exec and Global Configuration

Examples To show the public key generated for the user, use the command:

```
awplus# show crypto key userkey manager
```

To store the RSA public key generated for the user manager to the file "user.pub", use the command:

```
awplus# show crypto key userkey manager rsa > manager-rsa.pub
```

Output Figure 29-4: Example output from the **show crypto key userkey** command

```
Type Bits   Fingerprint
-----------------------------------------------------------
rsa  2048   e8:d6:1b:c0:f4:b6:e6:7d:02:2e:a9:d4:a1:ca:3b:11
rsa1 1024   12:25:60:95:64:08:8e:a1:8c:3c:45:1b:44:b9:33:9b
```

Table 4: Parameters in the output of the **show crypto key userkey** command

Parameter	Description
Type	The algorithm used to generate the key.
Bits	Length in bits of the key.
Fingerprint	Checksum value for the key.

Related commands crypto key generate userkey

show running-config ssh

Overview This command displays the current running configuration of Secure Shell (SSH).

Syntax

```
show running-config ssh
```

Mode Privileged Exec and Global Configuration

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

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

Output Figure 29-5: Example output from the **show running-config ssh** command

```
!
ssh server session-timeout 600
ssh server login-timeout 30
ssh server allow-users manager 192.168.1.*
ssh server allow-users john
ssh server deny-user john*.a-company.com
ssh server
```

Table 5: Parameters in the output of the **show running-config ssh** command

Parameter	Description
`ssh server`	SSH server is enabled.
`ssh server v2`	SSH server is enabled and only support SSHv2.
`ssh server<port>`	SSH server is enabled and listening on the specified TCP port.
`no ssh server scp`	SCP service is disabled.
`no ssh server sftp`	SFTP service is disabled.
`ssh server session-timeout`	Configure the server session timeout.
`ssh server login-timeout`	Configure the server login timeout.
`ssh server max-startups`	Configure the maximum number of concurrent sessions waiting authentication.
`no ssh server authentication password`	Password authentication is disabled.
`no ssh server authentication publickey`	Public key authentication is disabled.

Table 5: Parameters in the output of the **show running-config ssh** command

Parameter	Description
`ssh server allow-users`	Add the user (and hostname) to the allow list.
`ssh server deny-users`	Add the user (and hostname) to the deny list.

Related commands

service ssh

show ssh server

show ssh

Overview This command displays the active SSH sessions on the device, both incoming and outgoing.

Syntax

```
show ssh
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the current SSH sessions on the device, use the command:

```
awplus# show ssh
```

Output Figure 29-6: Example output from the **show ssh** command

```
Secure Shell Sessions:
ID  Type Mode   Peer Host    Username   State       Filename
-----------------------------------------------------------------
414 ssh  server 172.16.23.1  root       open
456 ssh  client 172.16.23.10 manager    user-auth
459 scp  client 172.16.23.12 root       download    example.awd
463 ssh  client 5ffe:33fe:5632:ffbb:bc35:ddee:0101:ac51
                             manager    user-auth
```

Table 6: Parameters in the output of the **show ssh** command

Parameter	Description
ID	Unique identifier for each SSH session.
Type	Session type; either SSH, SCP, or SFTP.
Mode	Whether the device is acting as an SSH client (client) or SSH server (server) for the specified session.
Peer Host	The hostname or IP address of the remote server or client.
Username	Login user name of the server.

Table 6: Parameters in the output of the **show ssh** command (cont.)

Parameter	Description	
State	The current state of the SSH session. One of:	
	connecting	The device is looking for a remote server.
	connected	The device is connected to the remote server.
	accepted	The device has accepted a new session.
	host-auth	host-to-host authentication is in progress.
	user-auth	User authentication is in progress.
	authenticated	User authentication is complete.
	open	The session is in progress.
	download	The user is downloading a file from the device.
	upload	The user is uploading a file from the device.
	closing	The user is terminating the session.
	closed	The session is closed.
Filename	Local filename of the file that the user is downloading or uploading.	

Related commands clear ssh

show ssh client

Overview This command displays the current configuration of the Secure Shell client.

Syntax

```
show ssh client
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the current configuration for SSH clients on the login shell, use the command:

```
awplus# show ssh client
```

Output Figure 29-7: Example output from the **show ssh client** command

```
Secure Shell Client Configuration
-----------------------------------------------------------------
Port                            : 22
Version                         : 2,1
Connect Timeout                 : 30 seconds
Session Timeout                 : 0 (off)
Debug                           : NONE
```

Table 7: Parameters in the output of the **show ssh client** command

Parameter	Description
Port	SSH server TCP port where the SSH client connects to. The default is port 22.
Version	SSH server version, either "2" or "2,1". From AlliedWare Plus 5.5.1-1.1 onwards, SSH version 1 is not supported.
Connect Timeout	Time in seconds that the SSH client waits for an SSH session to establish. If the value is 0, the connection is terminated when it reaches the TCP timeout.
Debug	Whether debugging is active on the client.

Related commands show ssh server

Command changes Version 5.5.3-1.1: added to AR1050V

show ssh server

Overview This command displays the current configuration of the Secure Shell server.

Note that changes to the SSH configuration affects only new SSH sessions coming from remote hosts, and does not affect existing sessions.

Syntax

```
show ssh server
```

Mode User Exec, Privileged Exec, and Global Configuration

Example To display the current configuration of the Secure Shell server, use the command:

```
awplus# show ssh server
```

Output Figure 29-8: Example output from the **show ssh server** command

```
Secure Shell Server Configuration
------------------------------------------------------------------------------
SSH Server                          : Enabled
Protocol                            : IPv4,IPv6
Port                                : 22
Version                             : 2
Services                            : scp, sftp
User Authentication                 : publickey, password
Resolve Hosts                       : Disabled
Session Timeout                     : 0 (Off)
Login Timeout                       : 60 seconds
Maximum Authentication Tries        : 6
Maximum Startups                    : 10
Debug                               : NONE
Ciphers                             : aes128-cbc,aes128-ctr,aes192-ctr,aes256-ctr
KEX                                 : curve25519-sha256@libssh.org,
                                      ecdh-sha2-nistp256,ecdh-sha2-nistp384,
                                      ecdh-sha2-nistp521,
                                      diffie-hellman-group-exchange-sha256,
                                      diffie-hellman-group-exchange-sha1,
                                      diffie-hellman-group14-sha1
```

Table 8: Parameters in the output of the **show ssh server** command

Parameter	Description
SSH Server	Whether the Secure Shell server is enabled or disabled.
Port	TCP port where the Secure Shell server listens for connections. The default is port 22.
Version	SSH server version; either '2' or '2,1'. From AlliedWare Plus 5.5.1-1.1 onwards, SSH version 1 is not supported.
Services	List of the available Secure Shell services; one or more of SHELL, SCP or SFTP.

Table 8: Parameters in the output of the **show ssh server** command (cont.)

Parameter	Description
`User Authentication`	List of available authentication methods.
`Login Timeout`	Time (in seconds) that the SSH server will wait the SSH session to establish. If the value is 0, the client login will be terminated when TCP timeout reaches.
`Idle Timeout`	Time (in seconds) that the SSH server will wait to receive data from the SSH client. The server disconnects if this timer limit is reached. If set at 0, the idle timer remains off.
`Maximum Startups`	The maximum number of concurrent connections that are waiting authentication. The default is 10.
`Debug`	Whether debugging is active on the server.
`Ciphers`	List of ciphers permitted.
`KEX`	List of available Key Exchange algorithms.

Related commands

show ssh

show ssh client

show ssh server allow-users

Overview This command displays the user entries in the allow list of the SSH server.

Syntax

```
show ssh server allow-users
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the user entries in the allow list of the SSH server, use the command:

```
awplus# show ssh server allow-users
```

Output Figure 29-9: Example output from the **show ssh server allow-users** command

```
Username          Remote Hostname (pattern)
----------------- ------------------------------
awplus            192.168.*
john
manager           *.alliedtelesis.com
```

Table 9: Parameters in the output of the **show ssh server allow-users** command

Parameter	Description
`Username`	User name that is allowed to access the SSH server.
`Remote Hostname (pattern)`	IP address or hostname pattern of the remote client. The user is allowed requests from a host that matches this pattern. If no hostname is specified, the user is allowed from all hosts.

Related commands

ssh server allow-users

ssh server deny-users

show ssh server deny-users

Overview This command displays the user entries in the deny list of the SSH server. The user in the deny list is rejected to access the SSH server. If a user is not included in the access list of the SSH server, the user is also rejected.

Syntax

```
show ssh server deny-users
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the user entries in the deny list of the SSH server, use the command:

```
awplus# show ssh server deny-users
```

Output Figure 29-10: Example output from the **show ssh server deny-users** command

```
Username          Remote Hostname (pattern)
----------------- --------------------------------
john              *.b-company.com
manager           192.168.2.*
```

Table 10: Parameters in the output of the **show ssh server deny-user** command

Parameter	Description
`Username`	The user that this rule applies to.
`Remote Hostname (pattern)`	IP address or hostname pattern of the remote client. The user is denied requests from a host that matches this pattern. If no hostname is specified, the user is denied from all hosts.

Related commands

ssh server allow-users

ssh server deny-users

ssh

Overview Use this command to initiate a Secure Shell connection to a remote SSH server.

If the server requests a password to login, you need to type in the correct password at the "Password:" prompt.

An SSH client identifies the remote SSH server by its public key registered on the client device. If the server identification is changed, server verification fails. If the public key of the server has been changed, the public key of the server must be explicitly added to the known host database.

NOTE: *A hostname specified with SSH cannot begin with a hyphen (-) character.*

Syntax

```
ssh [ip|ipv6] [user <username>|port <1-65535>|version 2]
<remote-device> [<command>]
```

Parameter	Description
`ip`	Specify IPv4 SSH.
`ipv6`	Specify IPv6 SSH.
`user`	Login user. If user is specified, the username is used for login to the remote SSH server when user authentication is required. Otherwise the current user name is used.
	<username> User name to login on the remote server.
`port`	SSH server port. If port is specified, the SSH client connects to the remote SSH server with the specified TCP port. Otherwise, the client port configured by "ssh client" command or the default TCP port (22) is used.
	<1-65535> TCP port.
`version`	SSH client version. From 5.5.1-1.1 onwards, SSH only supports version 2.
<remote-device>	IPv4/IPv6 address or hostname of a remote server. The address is in the format A.B.C.D for an IPv4 address, or in the format X:X::X:X for an IPv6 address. Note that a hostname specified with SSH cannot begin with a hyphen (-) character.
<command>	A command to execute on the remote server. If a command is specified, the command is executed on the remote SSH server and the session is disconnected when the remote command finishes.

Mode User Exec and Privileged Exec

Examples To login to the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 as user 'manager', use the command:

```
awplus# ssh ip user manager 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 that is listening on TCP port 2000, use the command:

```
awplus# ssh port 2000 192.0.2.5
```

To login to the remote SSH server 'example_host' using an IPv6 session, use the command:

```
awplus# ssh ipv6 example_host
```

To run the **cmd** command on the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5 cmd
```

Related commands

crypto key generate userkey

crypto key pubkey-chain knownhosts

debug ssh client

ssh client

Command changes

Version 5.5.3-1.1: added to AR1050V

Version 5.5.1-1.1: support removed for SSH protocol v1

Version 5.4.8-2.1: secure mode syntax added for x950, SBx908 GEN2.

Version 5.4.8-1.2: secure mode syntax added for x220, x930, x550, XS900MX.

Version 5.4.6-2.1: VRF-lite support added for AR-Series devices.

ssh client

Overview This command modifies the default configuration parameters of the Secure Shell (SSH) client. The configuration is used for any SSH client on the device to connect to remote SSH servers. Any parameters specified on SSH client explicitly override the default configuration parameters.

The change affects the current user shell only. When the user exits the login session, the configuration does not persist. This command does not affect existing SSH sessions.

The **no** variant of this command resets configuration parameters of the Secure Shell (SSH) client changed by the ssh client command, and restores the defaults.

This command does not affect the existing SSH sessions.

Syntax

```
ssh client {port <1-65535>|version 2|session-timeout
<0-3600>|connect-timeout <1-600>}
```

```
no ssh client {port|version|session-timeout|connect-timeout}
```

Parameter	Description
`port`	The default TCP port of the remote SSH server. If an SSH client specifies an explicit port of the server, it overrides the default TCP port. Default: 22
	<1-65535> TCP port number.
`version`	The SSH version used by the client for SSH sessions. From 5.5.1-1.1 onwards, the SSH client supports only version 2
`session-timeout`	The global session timeout for SSH sessions. If the session timer lapses since the last time an SSH client received data from the remote server, the session is terminated. If the value is 0, then the client does not terminate the session. Instead, the connection is terminated when it reaches the TCP timeout. 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. Default: 30
	<1-600> Timeout in seconds.

Mode Privileged Exec

Examples To configure the default TCP port for SSH clients to 2200, and the session timer to 10 minutes, use the command:

```
awplus# ssh client port 2200 session-timeout 600
```

To configure the connect timeout of SSH client to 10 seconds, use the command:

```
awplus# ssh client connect-timeout 10
```

To restore the connect timeout to its default, use the command:

```
awplus# no ssh client connect-timeout
```

Related commands

show ssh client

ssh

Command changes

Version 5.5.3-1.1: added to AR1050V

Version 5.5.2-1.1: **vrf** parameter added for products that support VRF

Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

ssh client allow-legacy-ssh-rsa

Overview Use this command to enable support for the legacy ssh-rsa algorithm on the SSH client. Support for this algorithm was removed in version 5.5.1-1.1 due to security concerns. Support for it is still disabled by default and you should only enable it if you cannot avoid using ssh-rsa. It cannot be enabled when the device is in Secure Mode.

Use the **no** variant of this command to disable support for the legacy ssh-rsa algorithm on the SSH client.

Syntax

```
ssh client allow-legacy-ssh-rsa
no ssh client allow-legacy-ssh-rsa
```

Default Disabled

Mode Global Configuration

Example To enable SSH client support for the legacy ssh-rsa algorithm, use the commands:

```
awplus# configure terminal
awplus(config)# ssh client allow-legacy-ssh-rsa
```

Related commands

show ssh client

ssh client

ssh server allow-legacy-ssh-rsa

Command changes

Version 5.5.3-1.1: added to AR1050V

Version 5.5.3-0.1: command added

ssh server

Overview Use this command to modify the configuration of the SSH server. Changing these parameters affects new SSH sessions connecting to the device.

Use the **no** variant of this command to restore the configuration of a specified parameter to its default. The change affects the SSH server immediately if the server is running. Otherwise, the configuration is used when the server starts.

To enable the SSH server, use the service ssh command.

Syntax

```
ssh server <1-65535>
ssh server {[session-timeout <0-3600>] [login-timeout <1-600>]
[max-startups <1-128>]}
no ssh server {[session-timeout] [login-timeout]
[max-startups]}
```

Parameter	Description
<1-65535>	The TCP port number that the server listens to for incoming SSH sessions. Default: 22
`session-timeout`	The maximum time period that the server waits before deciding that a session is inactive and should be terminated. The server considers the session inactive when it has not received any data from the client, and when the client does not respond to keep alive messages. Default: 0 (session timer remains off).
	Enter a timeout between 0-3600 seconds.
`login-timeout`	The maximum time period the server waits before disconnecting an unauthenticated client. Default: 60
	Enter a timeout between 1- 600 seconds.
`max-startups`	The maximum number of concurrent unauthenticated connections the server accepts. When the number of SSH connections awaiting authentication reaches the limit, the server drops any additional connections until authentication succeeds or the login timer expires for a connection. Default: 10
	Enter a number of sessions in the range of 1-128.

Mode Global Configuration

Examples To set the session timer of the SSH server to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server session-timeout 600
```

To set the login timeout of the SSH server to 30 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 30
```

To limit the number of SSH client connections waiting for authentication from the SSH server to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-startups 3
```

To return the limit on the number of waiting connections to the default of 10, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server max-startups
```

To support the SSH server with TCP port 2200, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server 2200
```

Related commands

show ssh server

ssh client

Command changes

Version 5.5.1-1.1: support removed for the ssh-rsa algorithm in OpenSSH and for SSH protocol v1

ssh server allow-legacy-ssh-rsa

Overview Use this command to enable support for the legacy ssh-rsa algorithm on the SSH server. Support for this algorithm was removed in version 5.5.1-1.1 due to security concerns. Support for it is still disabled by default and you should only enable it if you cannot avoid using ssh-rsa. It cannot be enabled when the device is in Secure Mode.

Use the **no** variant of this command to disable support for the legacy ssh-rsa algorithm on the SSH server.

Syntax

```
ssh server allow-legacy-ssh-rsa
no ssh server allow-legacy-ssh-rsa
```

Default Disabled

Mode Global Configuration

Example To enable SSH server support for the legacy ssh-rsa algorithm, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-legacy-ssh-rsa
```

Related commands show ssh server

ssh server

ssh client allow-legacy-ssh-rsa

Command changes Version 5.5.3-0.1: command added

ssh server allow-users

Overview This command adds a username pattern to the allow list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is accepted.

When there are no registered users in the server's database of allowed users, the SSH server does not accept SSH sessions even when enabled.

SSH server also maintains the deny list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

The **no** variant of this command deletes a username pattern from the allow list of the SSH server. To delete an entry from the allow list, the username and hostname pattern should match exactly with the existing entry.

Syntax

```
ssh server allow-users <username-pattern> [<hostname-pattern>]
no ssh server allow-users <username-pattern>
[<hostname-pattern>]
```

Parameter	Description
<username-pattern>	The username pattern that users can match to. An asterisk acts as a wildcard character that matches any string of characters.
<hostname-pattern>	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
<username-pattern>	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.
<hostname-pattern>	The host name pattern that hosts can match to. If specified, the server denies the user only when they connect from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters.

Mode Global Configuration

Examples To deny the user `john` to access SSH login from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john
```

To deny the user john to access SSH login from a range of IP address (from 192.168.2.1 to 192.168.2.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john 192.168.2.*
```

To deny the user `john` to access SSH login from `b-company.com` domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john*.b-company.com
```

To delete the existing user entry `john 192.168.2.*` in the deny list, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server deny-users john 192.168.2.*
```

Related commands

show running-config ssh

show ssh server deny-users

ssh server allow-users

ssh server max-auth-tries

Overview Use this command to specify the maximum number of SSH authentication attempts that the device will allow.

Use the **no** variant of this command to return the maximum number of attempts to its default value of 6.

Syntax

```
ssh server max-auth-tries <1-32>
no ssh server max-auth-tries
```

Parameter	Description
<1-32>	Maximum number of SSH authentication attempts the device will allow.

Default 6 attempts

Mode Global Configuration

Usage By default, users must wait one second after a failed login attempt before trying again. You can increase this gap by using the command aaa login fail-delay.

Example To set the maximum number of SSH authentication attempts to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-auth-tries 3
```

Related commands show ssh server

ssh server resolve-host

Overview This command enables resolving an IP address from a host name using a DNS server for client host authentication.

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

Syntax

```
ssh server resolve-hosts
no ssh server resolve-hosts
```

Default This feature is disabled by default.

Mode Global Configuration

Usage notes Your device has a DNS Client that is enabled automatically when you add a DNS server to your device.

Example To resolve a host name using a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server resolve-hosts
```

Related commands

ip name-server

show ssh server

ssh server allow-users

ssh server deny-users

ssh server scp

Overview This command enables the Secure Copy (SCP) service on the SSH server. Once enabled, the server accepts SCP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SCP connections. The SCP service is enabled by default as soon as the SSH server is enabled.

The **no** variant of this command disables the SCP service on the SSH server. Once disabled, SCP requests from remote clients are rejected.

Syntax

```
ssh server scp
no ssh server scp
```

Mode Global Configuration

Examples To enable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server scp
```

To disable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server scp
```

Related commands show running-config ssh

show ssh server

ssh server secure-algs

Overview Use this command to force the SSH server to only use ciphers, key exchange algorithms and Message Authentication Code (MAC) algorithms that are currently considered best-practice.

This command is the same as using all of the commands ssh server secure-ciphers, ssh server secure-hostkey, ssh server secure-mac, and ssh server secure-kex. However, it does not include the optional **exclude-nist-curves** parameter of ssh server secure-kex.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of algorithms.

Syntax

```
ssh server secure-algs
no ssh server secure-algs
```

Default Disabled.

Mode Global Configuration

Usage notes To see the list of algorithms, use the show ssh server command.

Example To force the SSH server to use best-practice algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-algs
```

Related commands

show ssh server

ssh server

ssh server secure-ciphers

ssh server secure-hostkey

ssh server secure-kex

ssh server secure-mac

Command changes Version 5.5.1-1.1: command added

ssh server secure-ciphers

Overview Use this command to force the SSH server to only negotiate ciphers regarded as current best-practice.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of ciphers.

Syntax

```
ssh server secure-ciphers
no ssh server secure-ciphers
```

Default Not set

Mode Global Configuration

Usage notes To see the list of ciphers, use the show ssh server command.

Example To configure the SSH server to use best-practice ciphers, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-ciphers
```

Related commands

show ssh server

ssh server

ssh server secure-algs

ssh server secure-hostkey

ssh server secure-kex

ssh server secure-mac

Command changes Version 5.5.0-1.1: command added

ssh server secure-hostkey

Overview Use this command to force the SSH server to only use hostkey algorithms that are currently considered best-practice. This excludes NIST curve-based hostkey algorithms.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of hostkey algorithms.

Syntax
```
ssh server secure-hostkey
no ssh server secure-hostkey
```

Default Disabled

Mode Global Configuration

Usage notes Using this command may reduce compatibility with older SSH clients.

To see the list of hostkey algorithms, use the show ssh server command.

Example To force the SSH server to use best-practice hostkey algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-hostkey
```

Related commands
show ssh server

ssh server

ssh server secure-algs

ssh server secure-ciphers

ssh server secure-kex

ssh server secure-mac

Command changes Version 5.5.2-2.1: command added

ssh server secure-kex

Overview Use this command to force the SSH server to only use key exchange algorithms that are currently considered best-practice.

For example, using this command stops the device from using the diffie-hellman-group-exchange-sha1 key exchange algorithm.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of key-exchange algorithms.

Syntax

```
ssh server secure-kex [exclude-nist-curves]
no ssh server secure-kex
```

Parameter	Description
`exclude-nist-curves`	Also exclude all NIST key exchange algorithms. Using this parameter may reduce compatibility with older SSH clients.

Default Disabled.

Mode Global Configuration

Usage notes To see the list of key exchange algorithms, use the show ssh server command.

Example To force the SSH server to use best-practice key-exchange algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-kex
```

Related commands

show ssh server

ssh server

ssh server secure-algs

ssh server secure-ciphers

ssh server secure-hostkey

ssh server secure-mac

Command changes Version 5.5.2-2.1: **exclude-nist-curves** parameter added

Version 5.5.0-2.3: command added

ssh server secure-mac

Overview Use this command to force the SSH server to only use Message Authentication Code (MAC) algorithms that are currently considered best-practice.

Use the **no** variant of this command to stop forcing the SSH server to use this restricted set of MAC algorithms.

Syntax

```
ssh server secure-mac
no ssh server secure-mac
```

Default Disabled.

Mode Global Configuration

Usage notes To see the list of MAC algorithms, use the show ssh server command.

Example To force the SSH server to use best-practice MAC algorithms, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server secure-mac
```

Related commands

show ssh server

ssh server

ssh server secure-algs

ssh server secure-ciphers

ssh server secure-hostkey

ssh server secure-kex

Command changes Version 5.5.1-1.1: command added

ssh server sftp

Overview This command enables the Secure FTP (SFTP) service on the SSH server. Once enabled, the server accepts SFTP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SFTP connections. The SFTP service is enabled by default as soon as the SSH server is enabled. If the SSH server is disabled, SFTP service is unavailable.

The **no** variant of this command disables SFTP service on the SSH server. Once disabled, SFTP requests from remote clients are rejected.

Syntax

```
ssh server sftp
no ssh server sftp
```

Mode Global Configuration

Examples To enable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server sftp
```

To disable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server sftp
```

Related commands show running-config ssh

show ssh server

ssh server tcpforwarding

Overview Use this command to enable TCP port forwarding on the SSH server. It is disabled by default, to enhance security.

Use the **no** variant of this command to disable TCP port forwarding again.

Syntax

```
ssh server tcpforwarding
no ssh server tcpforwarding
```

Default Disabled

Mode Global Configuration

Example To enable TCP port forwarding, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server tcpforwarding
```

To disable it again, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server tcpforwarding
```

Related commands show ssh server

Command changes Version 5.5.2-1.1: command added

undebug ssh client

Overview This command applies the functionality of the **no** debug ssh client command.

Command changes Version 5.5.3-1.1: added to AR1050V

undebug ssh server

Overview This command applies the functionality of the **no** debug ssh server command.

30 Trigger Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure Triggers. For more information, see the Triggers Feature Overview and Configuration Guide.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Command List

- "active (trigger)" on page 1013
- "day" on page 1014
- "debug trigger" on page 1016
- "description (trigger)" on page 1017
- "repeat" on page 1018
- "script" on page 1019
- "show debugging trigger" on page 1021
- "show running-config trigger" on page 1022
- "show trigger" on page 1023
- "test" on page 1028
- "time (trigger)" on page 1029
- "trap" on page 1031
- "trigger" on page 1032
- "trigger activate" on page 1033
- "type atmf guest" on page 1034
- "type atmf node" on page 1035
- "type cpu" on page 1037
- "type interface" on page 1038

- "type linkmon-probe" on page 1039
- "type log" on page 1041
- "type memory" on page 1042
- "type periodic" on page 1043
- "type ping-poll" on page 1044
- "type reboot" on page 1045
- "type time" on page 1046
- "undebug trigger" on page 1047

active (trigger)

Overview This command enables a trigger. This allows the trigger to activate when its trigger conditions are met.

The **no** variant of this command disables a trigger. While in this state the trigger cannot activate when its trigger conditions are met.

Syntax

```
active
no active
```

Default Active, which means that triggers are enabled by default

Mode Trigger Configuration

Usage notes Configure a trigger first before you use this command to activate it.

For information about configuring a trigger, see the Triggers_Feature Overview and Configuration Guide.

Examples To enable trigger 172, so that it can activate when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 172
awplus(config-trigger)# active
```

To disable trigger 182, preventing it from activating when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 182
awplus(config-trigger)# no active
```

Related commands

show trigger

trigger

trigger activate

day

Overview This command specifies the days or date that the trigger can activate on. You can specify one of:

- A specific date
- A specific day of the week
- A list of days of the week
- A day of any month of any year
- A day of a specific month in any year
- Every day

By default, the trigger can activate on any day.

Syntax

```
day every-day
day <1-31>
day <1-31> <month>
day <1-31> <month> <year>
day <weekday>
```

Parameter	Description
`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: **january, february, march, april, may, june, july, august, september, october, november**, and **december**.
<year>	Sets the year that the trigger is permitted to activate in, between 2000 and 2035.
<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: **monday, tuesday, wednesday, thursday, friday, saturday**, and **sunday**.

Default **every-day**, so by default, the trigger can activate on any day.

Mode Trigger Configuration

Usage notes For example trigger configurations that use the **day** command, see "Restrict Internet Access" and "Turn off Power to Port LEDs" in the Triggers Feature Overview and Configuration Guide.

Examples

To permit trigger 55 to activate on the 1 June 2019, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 55
awplus(config-trigger)# day 1 jun 2019
```

To permit trigger 12 to activate on Mondays, Wednesdays and Fridays, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# day monday wednesday friday
```

To permit trigger 17 to activate on the 5th day of any month, in any year, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 17
awplus(config-trigger)# day 5
```

To permit trigger 6 to activate on the 20th day of September, in any year, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 6
awplus(config-trigger)# day 20 september
```

To permit trigger 14 to activate on the 1st day of each month, in any year, at 11.00am, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 14
awplus(config-trigger)# day 1
awplus(config-trigger)# type time 11:00
```

Related commands

show trigger

type time

trigger

Command changes

Version 5.4.8-2.1: day of the month functionality added

debug trigger

Overview This command enables trigger debugging. This generates detailed messages about how your device is processing the trigger commands and activating the triggers.

The **no** variant of this command disables trigger debugging.

Syntax

```
debug trigger
no debug trigger
```

Mode Privilege Exec

Examples To start trigger debugging, use the command:

```
awplus# debug trigger
```

To stop trigger debugging, use the command:

```
awplus# no trigger
```

Related commands

show debugging trigger

show trigger

test

trigger

undebug trigger

description (trigger)

Overview This command adds an optional description to help you identify the trigger. This description is displayed in show command outputs and log messages.

The **no** variant of this command removes a trigger's description. The show command outputs and log messages stop displaying a description for this trigger.

Syntax

```
description <description>
no description
```

Parameter	Description
<description>	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.
<1-4292967294>	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 30-1: 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
```

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 30-1: Example output from **show trigger**

```
awplus#show trigger
TR# Type & Details       Name                 Ac Te Repeat      #Scr Days/Date
-------------------------------------------------------------------------------
001 CPU (80% any)        Busy CPU             Y  N  5            1   smtwtfs
005 Periodic (30 min)    Regular status check Y  N  Continuous   1   -mtwtf-
007 Memory (85% up)      High mem usage       Y  N  8            1   smtwtfs
011 Time (00:01)         Weekend access       Y  N  Continuous   1   ------s
013 Reboot                                    Y  N  Continuous   2   smtwtfs
019 Ping-poll (5 up)     Connection to svr1   Y  N  Continuous   1   smtwtfs
-------------------------------------------------------------------------------
```

Table 30-2: Parameters in the output of **show trigger**

Parameter	Description
`TR#`	Trigger identifier (ID).
`Type & Details`	The trigger type, followed by the trigger details in brackets.
`Name`	Descriptive name of the trigger configured with the description (trigger) command.
`Ac`	Whether the trigger is active (Y), or inactive (N).
`Te`	Whether the trigger is in test mode (Y) or not (N).

Table 30-2: Parameters in the output of **show trigger** (cont.)

Parameter	Description
Repeat	Whether the trigger repeats continuously, and if not, the configured repeat count for the trigger. To see the number of times a trigger has activated, use the **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 30-2: Example output from **show trigger** for a specific trigger

```
awplus#show trigger 1
Trigger Configuration Details
-------------------------------------------------------------
Trigger ..................... 1
Name ........................ display cpu usage when pass 80%
Type and details ............ CPU (80% up)
Days ........................ smtwtfs
Active ...................... Yes
Test ........................ No
Trap ........................ Yes
Repeat ...................... Continuous
Modified .................... Fri Feb 3 17:18:44 2017
Number of activations ....... 0
Last activation ............. not activated
Number of scripts ........... 1
1. shocpu.scp
2.
3.
4.
5.
-------------------------------------------------------------
```

To display detailed information about all triggers, use the command:

```
awplus# show trigger full
```

Table 30-3: Example output from **show trigger full**

```
awplus#show trigger full
Trigger Configuration Details
 ------------------------------------------------------------
Trigger ..................... 1
Name ........................ Busy CPU
Type and details ............ CPU (80% up)
Days ........................ smtwtfs
Active ...................... Yes
Test ........................ No
Trap ........................ Yes
Repeat ...................... Continuous
Modified .................... Fri Feb 3 17:05:16 2017
Number of activations ....... 0
Last activation ............. not activated
Number of scripts ........... 2
  1. flash:/cpu_alert.sh
  2. flash:/reconfig.scp
  3.
  4.
  5.
Trigger ..................... 5
Name ........................ Regular status check
Type and details ............ Periodic (30 min)
Days ........................ smtwtfs
Active ...................... Yes
Test ........................ No
Trap ........................ Yes
Repeat ...................... 5 (2)
Modified .................... Fri Feb 3 17:18:44 2017
Number of activations ....... 0
Last activation ............. Fri Feb 10 18:00:00 2017
Number of scripts ........... 1
  1. flash:/stat_check.scp
  2.
  3.
  4.
  5.
------------------------------------------------------------
```

Table 31: Parameters in the output of **show trigger full** and **show trigger** for a specific trigger

Parameter	Description
`Trigger`	The ID of the trigger.
`Name`	Descriptive name of the trigger.
`Type and details`	The trigger type and its activation conditions.
`Days`	The days on which the trigger is permitted to activate.

Table 31: Parameters in the output of **show trigger full** and **show trigger** for a specific trigger (cont.)

Parameter	Description
Date	The date on which the trigger is permitted to activate. Only displayed if configured, in which case it replaces "Days".
Active	Whether or not the trigger is permitted to activate.
Test	Whether or not the trigger is operating in diagnostic mode.
Trap	Whether or not the trigger is enabled to send SNMP traps.
Repeat	Whether the trigger repeats an unlimited number of times (Continuous) or for a set number of times. When the trigger can repeat only a set number of times, then the number of times the trigger has been activated is displayed in brackets.
Modified	The date and time of the last time that the trigger was modified.
Number of activations	Number of times the trigger has been activated since the last restart of the device.
Last activation	The date and time of the last time that the trigger was activated.
Number of scripts	How many scripts are associated with the trigger, followed by the names of the script files in the order in which they run.

To display counter information about all triggers use the command:

```
awplus# show trigger counter
```

Figure 30-3: Example output from **show trigger counter**

```
awplus# show trigger counter
Trigger Module Counters
-------------------------------------------------------
Trigger activations                              4
Last trigger activated                          55
Time triggers activated today                    0
Periodic triggers activated today                0
Interface triggers activated today               1
CPU triggers activated today                     2
Memory triggers activated today                  1
Reboot triggers activated today                  0
Ping-poll triggers activated today               0
USB event triggers activated today               0
Stack master fail triggers activated today       0
Stack member triggers activated today            0
Stack link triggers activated today              0
ATMF node triggers activated today               0
ATMF guest triggers activated today              0
Log triggers activated today                     0
-------------------------------------------------------
```

Related commands

active (trigger)

debug trigger

script

trigger

trigger activate

test

Overview This command puts the trigger into a diagnostic mode. In this mode the trigger may activate but when it does it will not run any of the trigger's scripts. A log message will be generated to indicate when the trigger has been activated.

The **no** variant of this command takes the trigger out of diagnostic mode, restoring normal operation. When the trigger activates, the scripts associated with the trigger will be run, as normal.

Syntax

```
test
no test
```

Mode Trigger Configuration

Usage notes Configure a trigger first before you use this command to diagnose it. For information about configuring a trigger, see the Triggers_Feature Overview and Configuration Guide.

Examples To put trigger 5 into diagnostic mode, where no scripts will be run when the trigger activates, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# test
```

To take trigger 205 out of diagnostic mode, restoring normal operation, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no test
```

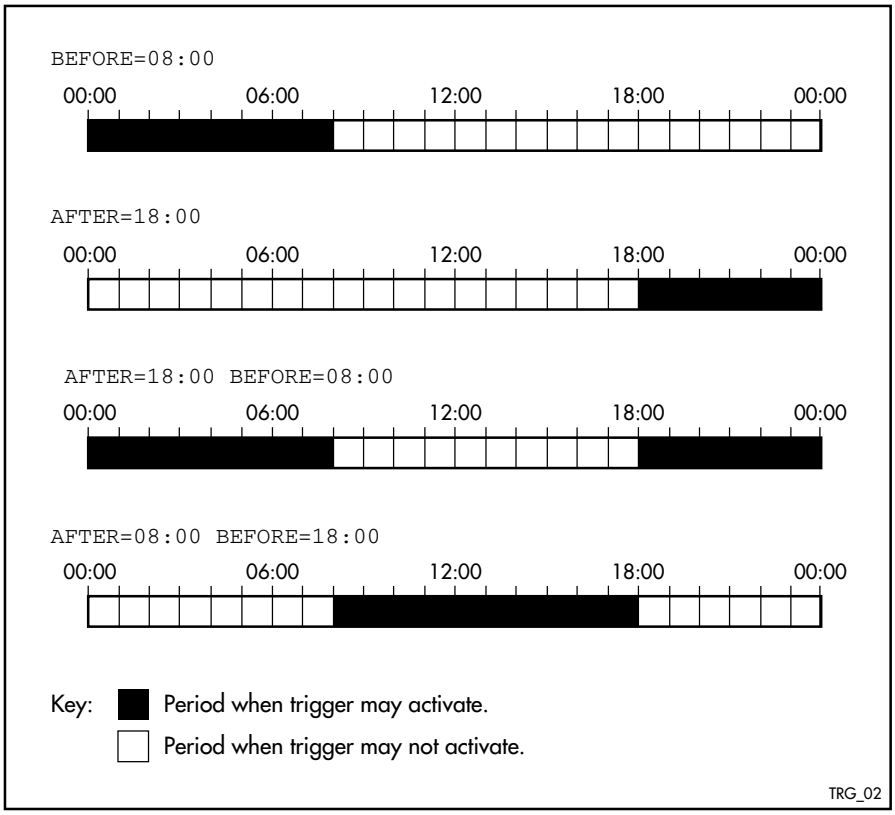
Related commands show trigger

trigger

time (trigger)

Overview This command specifies the time of day when the trigger is permitted to activate. The after parameter specifies the start of a time period that extends to midnight during which trigger may activate. By default the value of this parameter is 00:00:00 (am); that is, the trigger may activate at any time. The **before** parameter specifies the end of a time period beginning at midnight during which the trigger may activate. By default the value of this parameter is 23:59:59; that is, the trigger may activate at any time. If the value specified for **before** is later than the value specified for **after**, a time period from **"** after **"** to **"** before **"** is defined, during which the trigger may activate. This command is not applicable to time triggers (**type time**).

The following figure illustrates how the **before** and **after** parameters operate.



Syntax `time {[after <hh:mm:ss>] [before <hh:mm:ss>]}`

Parameter	Description
`after`*<hh:mm:ss>*	The earliest time of day when the trigger may be activated.
`before`*<hh:mm:ss>*	The latest time of day when the trigger may be activated.

Mode Trigger Configuration

Usage notes For example trigger configurations that use the **time (trigger)** command, see "Restrict Internet Access" and "Turn off Power to Port LEDs" in the Triggers Feature Overview and Configuration Guide.

Examples To allow trigger `63` to activate between midnight and 10:30am, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 63
awplus(config-trigger)# time before 10:30:00
```

To allow trigger `64` to activate between 3:45pm and midnight, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 64
awplus(config-trigger)# time after 15:45:00
```

To allow trigger `65` to activate between 10:30am and 8:15pm, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 65
awplus(config-trigger)# time after 10:30:00 before 20:15:00
```

Related commands show trigger

trigger

trap

Overview This command enables the specified trigger to send SNMP traps.

Use the **no** variant of this command to disable the sending of SNMP traps from the specified trigger.

Syntax

```
trap
no trap
```

Default SNMP traps are enabled by default for all defined triggers.

Mode Trigger Configuration

Usage notes You must configure SNMP before using traps with triggers. For more information, see:

- Support for Allied Telesis Enterprise_MIBs_in_AlliedWare Plus, for information about which MIB objects are supported.
- the SNMP Feature Overview and Configuration_Guide.
- the SNMP Commands chapter.

Since SNMP traps are enabled by default for all defined triggers, a common usage will be for the **no** variant of this command to disable SNMP traps from a specified trap if the trap is only periodic. Refer in particular to AT-TRIGGER-MIB in the Support for Allied Telesis Enterprise_MIBs_in AlliedWare Plus for further information about the relevant SNMP MIB.

Examples To enable SNMP traps to be sent from trigger 5, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# trap
```

To disable SNMP traps being sent from trigger 205, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no trap
```

Related commands trigger

show trigger

trigger

Overview This command is used to access the Trigger Configuration mode for the specified trigger. Once Trigger Configuration mode has been entered the trigger type information can be configured and the trigger scripts and other operational parameters can be specified. At a minimum the trigger type information must be specified before the trigger can become active.

The **no** variant of this command removes a specified trigger and all configuration associated with it.

Syntax

```
trigger <1-250>
no trigger <1-250>
```

Parameter	Description
<1-250>	A trigger ID.

Mode Global Configuration

Examples To enter trigger configuration mode for trigger 12, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 12
```

To completely remove all configuration associated with trigger 12, use the commands:

```
awplus# configure terminal
awplus(config)# no trigger 12
```

Related commands show trigger

trigger activate

trigger activate

Overview This command is used to manually activate a specified trigger from the Privileged Exec mode, which has been configured with the **trigger** command from the Global Configuration mode.

Syntax

```
trigger activate <1-250>
```

Parameter	Description
<1-250>	A trigger ID.

Mode Privileged Exec

Usage notes This command manually activates a trigger without the normal trigger conditions being met.

The trigger is activated even if it has been configured as inactive by using the command **no active**. The scripts associated with the trigger will be executed even if the trigger is in the diagnostic test mode.

Triggers activated manually do not have their repeat counts decremented or their 'last triggered' time updated, and do not result in updates to the '[type] triggers today' counters.

Example To manually activate trigger 12 use the command:

```
awplus# trigger activate 12
```

Related commands

active (trigger)

show trigger

trigger

type atmf guest

Overview This command configures a trigger to activate when an AMF guest node joins or leaves.

Syntax

```
type atmf guest {join|leave}
```

Parameter	Description
`join`	AMF guest node joins.
`leave`	AMF guest node leaves.

Mode Trigger Configuration

Example To configure trigger 86 to activate when an AMF guest node leaves, use the following commands:

```
awplus(config)# trigger 86
awplus(config-trigger)# type atmf guest leave
```

Related commands show trigger

Command changes Version 5.5.1-1.1: command added

type atmf node

Overview This command configures a trigger to activate when an AMF node joins or leaves.

Syntax

```
type atmf node {join|leave}
```

Parameter	Description
join	AMF node joins.
leave	AMF node leaves.

Mode Trigger Configuration

Example 1 To configure trigger 5 to activate when an AMF node leaves, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger)# type atmf node leave
```

Example 2 The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
====================
node1, node2, node3:
====================

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=======
node1:
=======

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
001 Periodic (2 min)   Periodic Status Chk  Y  N  Y Continuous  1   smtwtfs
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------

==============
Node2, Node3,
==============

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------
```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
========
Node1:
========

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!

============
Node2, Node3:
============

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

Related commands show trigger

type cpu

Overview This command configures a trigger to activate based on CPU usage level. Selecting the **up** option causes the trigger to activate when the CPU usage exceeds the specified usage level. Selecting the **down** option causes the trigger to activate when CPU usage drops below the specified usage level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

Syntax

```
type cpu <1-100> [up|down|any]
```

Parameter	Description
<1-100>	The percentage of CPU usage at which to trigger.
`up`	Activate when CPU usage exceeds the specified level.
`down`	Activate when CPU usage drops below the specified level
`any`	Activate when CPU usage passes the specified level in either direction

Mode Trigger Configuration

Usage notes For an example trigger configuration that uses the **type cpu** command, see "Capture Unusual CPU and RAM Activity" in the Triggers Feature Overview and Configuration Guide.

Examples To configure trigger `28` to be a CPU trigger that activates when CPU usage exceeds 80% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 28
awplus(config-trigger)# type cpu 80 up
```

To configure trigger `5` to be a CPU trigger that activates when CPU usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65
```

or

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65 any
```

Related commands show trigger

trigger

type interface

Overview This command configures a trigger to activate based on the link status of an interface. The trigger can be activated when the interface becomes operational by using the **up** option, or when the interface closes by using the **down** option. The trigger can also be configured to activate when either one of these events occurs by using the **any** option.

Syntax

```
type interface <interface> {up|down|any}
```

Parameter	Description
<interface>	Interface name.
up	Activate when interface becomes operational.
down	Activate when the interface closes.
any	Activate when any interface link status event occurs.

Mode Trigger Configuration

Example To configure trigger 19 to be an interface trigger that activates when eth0 becomes operational, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 19
awplus(config-trigger)# type interface eth0 up
```

Related commands show trigger

trigger

type linkmon-probe

Overview Use this command to create a trigger that will run a script when a Link Health Monitoring probe reports that a link becomes “good”, “bad”, or “unreachable”.

Syntax

```
type linkmon-probe <probename> <profilename>
{good|bad|unreachable|any}
```

Parameter	Description
<probename>	The name of the Link Health Monitoring probe that will be used for executing the trigger.
<profilename>	The name of the Link Health Monitoring performance profile that will be used for determine if the Link Health Monitoring probe is good, bad, or unreachable.
`good`	If the Link Health Monitoring probe becomes 'good' according to the Link Health Monitoring performance profile then the trigger will be executed.
`bad`	If the Link Health Monitoring probe goes 'bad' according to the Link Health Monitoring performance profile then the trigger will be executed.
`unreachable`	If the Link Health Monitoring probe becomes 'unreachable' according to the Link Health Monitoring performance profile then the trigger will be executed.
`any`	If the Link Health Monitoring probe changes state according to the Link Health Monitoring performance profile then the trigger will be executed.

Mode Trigger Configuration

Example When the Link Health Monitoring probes sent to the “test-probe” destination no longer meet the performance profile “test-profile” the link will be deemed “bad”. To create a trigger that will run a script when a Link Health Monitoring probe is deemed “bad”, use the following commands:

```
awplus(config)# trigger 1
awplus(config-trigger)# script 1 link-bad.scp
awplus(config-trigger)# type linkmon-probe test-probe
test-profile bad
```

To create a trigger that will run a script when the link is deemed “good” again, use the following commands:

```
awplus(config)# trigger 2
awplus(config-trigger)# script 1 link-good.scp
awplus(config-trigger)# type linkmon-probe test-probe
test-profile good
```

Related commands trigger

Command changes Version 5.4.8-1.1: command added

type log

Overview Use this command to configure a trigger to activate based on the content of log messages matching a string or regular expression.

Syntax

```
type log <log-message-string>
```

Parameter	Description
<log-message-string>	A string or a regular expression (PCRE) to match a log message or part of a log message.

Default There is no type or log message string set by default.

Mode Trigger Configuration

Usage notes Log type triggers fully support regular expressions using PCRE (Perl-Compatible Regular Expression) syntax.

Only log messages of severity level notice or higher can activate a trigger.

Note that any command executed by the script will generate a log message with level notice, and will include '[SCRIPT]' before the command string. Therefore, if something in the script matches the configured log message trigger string, it will retrigger indefinitely.

Example To configure trigger 6 to activate when a log message of level notice or higher indicates that any port has 'failed', use the commands:

```
awplus# configure terminal
awplus(config)# trigger 6
awplus(config-trigger)# type log port.+ failed
```

Related commands show trigger

trigger

Command changes Version 5.4.7-2.1: command added

type memory

Overview This command configures a trigger to activate based on RAM usage level. Selecting the **up** option causes the trigger to activate when memory usage exceeds the specified level. Selecting the **down** option causes the trigger to activate when memory usage drops below the specified level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

Syntax

```
type memory <1-100> [up|down|any]
```

Parameter	Description
<1-100>	The percentage of memory usage at which to trigger.
`up`	Activate when memory usage exceeds the specified level.
`down`	Activate when memory usage drops below the specified level.
`any`	Activate when memory usage passes the specified level in either direction.

Mode Trigger Configuration

Examples To configure trigger `12` to be a memory trigger that activates when memory usage exceeds 50% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# type memory 50 up
```

To configure trigger `40` to be a memory trigger that activates when memory usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65
```

or

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65 any
```

Related commands show trigger

trigger

type periodic

Overview This command configures a trigger to be activated at regular intervals. The time period between activations is specified in minutes.

Syntax

```
type periodic <1-1440>
```

Parameter	Description
<1-1440>	The number of minutes between activations.

Mode Trigger Configuration

Usage notes A combined limit of 10 triggers of the type periodic and time can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or
periodic
```

For an example trigger configuration that uses the **type periodic** command, see "See Daily Statistics" in the Triggers_Feature Overview and Configuration Guide.

Example To configure trigger `44` to activate periodically at `10` minute intervals use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 44
awplus(config-trigger)# type periodic 10
```

Related commands show trigger

trigger

type ping-poll

Overview This command configures a trigger that activates when Ping Polling identifies that a target device's status has changed. This allows you to run a configuration script when a device becomes reachable or unreachable.

Syntax

```
type ping-poll <1-100> {up|down}
```

Parameter	Description
<1-100>	The ping poll ID.
`up`	The trigger activates when ping polling detects that the target is reachable.
`down`	The trigger activates when ping polling detects that the target is unreachable.

Mode Trigger Configuration

Example To configure trigger `106` to activate when ping poll `12` detects that its target device is now unreachable, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 106
awplus(config-trigger)# type ping-poll 12 down
```

Related commands show trigger

trigger

type reboot

Overview This command configures a trigger that activates when your device is rebooted.

Syntax

```
type reboot
```

Mode Trigger Configuration

Example To configure trigger `32` to activate when your device reboots, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 32
awplus(config-trigger)# type reboot
```

Related commands show trigger

trigger

type time

Overview This command configures a trigger that activates at a specified time of day.

Syntax

```
type time <hh:mm>
```

Parameter	Description
<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

undebug trigger

Overview This command applies the functionality of the **no** debug trigger command.

31 Ping-Polling Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure Ping Polling. For more information, see the Ping Polling Feature Overview and Configuration Guide.

For information on filtering and saving command output, see the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Table 31-1: 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 1050
- "clear ping-poll" on page 1051
- "critical-interval" on page 1052
- "debug ping-poll" on page 1053

- "description (ping-polling)" on page 1054
- "fail-count" on page 1055
- "ip (ping-polling)" on page 1056
- "length (ping-poll data)" on page 1057
- "normal-interval" on page 1058
- "ping-poll" on page 1059
- "sample-size" on page 1060
- "show counter ping-poll" on page 1062
- "show ping-poll" on page 1064
- "source-ip" on page 1068
- "timeout (ping polling)" on page 1070
- "up-count" on page 1071
- "undebug ping-poll" on page 1072

active (ping-polling)

Overview This command enables a ping-poll instance. The polling instance sends ICMP echo requests to the device with the IP address specified by the ip (ping-polling) command.

By default, polling instances are disabled. When a polling instance is enabled, it assumes that the device it is polling is unreachable.

The **no** variant of this command disables a ping-poll instance. The polling instance no longer sends ICMP echo requests to the polled device. This also resets all counters for this polling instance.

Syntax

```
active
no active
```

Mode Ping-Polling Configuration

Examples To activate the ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# active
```

To disable the ping-poll instance 43 and reset its counters, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no active
```

Related commands

debug ping-poll

ip (ping-polling)

ping-poll

show ping-poll

clear ping-poll

Overview This command resets the specified ping poll, or all ping poll instances. This clears the ping counters, and changes the status of polled devices to unreachable. The polling instance changes to the polling frequency specified with the critical-interval command. The device status changes to reachable once the device responses have reached the up-count.

Syntax

```
clear ping-poll {<1-100>|all}
```

Parameter	Description
<1-100>	A ping poll ID number. The specified ping poll instance has its counters cleared, and the status of the device it polls is changed to unreachable.
`all`	Clears the counters and changes the device status of all polling instances.

Mode Privileged Exec

Examples To reset the ping poll instance 12, use the command:

```
awplus# clear ping-poll 12
```

To reset all ping poll instances, use the command:

```
awplus# clear ping-poll all
```

Related commands

active (ping-polling)

ping-poll

show ping-poll

critical-interval

Overview This command specifies the time period in seconds between pings when the polling instance has not received a reply to at least one ping, and when the device is unreachable.

This command enables the device to quickly observe changes in state, and should be set to a much lower value than the normal-interval command.

The **no** variant of this command sets the critical interval to the default of one second.

Syntax

```
critical-interval <1-65536>
no critical-interval
```

Parameter	Description
<1-65536>	Time in seconds between pings, when the device has failed to a ping, or the device is unreachable.

Default The default is 1 second.

Mode Ping-Polling Configuration

Examples To set the critical interval to 2 seconds for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# critical-interval 2
```

To reset the critical interval to the default of one second for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# no critical-interval
```

Related commands

fail-count

normal-interval

sample-size

show ping-poll

timeout (ping polling)

up-count

debug ping-poll

Overview This command enables ping poll debugging for the specified ping-poll instance. This generates detailed messages about ping execution.

The **no** variant of this command disables ping-poll debugging for the specified ping-poll.

Syntax

```
debug ping-poll <1-100>
no debug ping-poll {<1-100>|all}
```

Parameter	Description
<1-100>	A unique ping poll ID number.
all	Turn off all ping-poll debugging.

Mode Privileged Exec

Examples To enable debugging for ping-poll instance 88, use the command:

```
awplus# debug ping-poll 88
```

To disable all ping poll debugging, use the command:

```
awplus# no debug ping-poll all
```

To disable debugging for ping-poll instance 88, use the command:

```
awplus# no debug ping-poll 88
```

Related commands

active (ping-polling)

clear ping-poll

ping-poll

show ping-poll

undebug ping-poll

description (ping-polling)

Overview This command specifies a string to describe the ping-polling instance. This allows the ping-polling instance to be recognized easily in show commands. Setting this command is optional.

By default ping-poll instances do not have a description.

Use the **no** variant of this command to delete the description set.

Syntax

```
description <description>
no description
```

Parameter	Description
<description>	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
<ip-address>	An IPv4 address in dotted decimal notation `A.B.C.D`
<ipv6-address>	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
<1-100>	Number of pings that determines critical and up counts.

Default The default is 5.

Mode Ping-Polling Configuration

Examples To set the sample-size to 50 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# sample-size 50
```

To reset sample-size to the default of 5 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no sample-size
```

Related commands

critical-interval

fail-count

normal-interval

ping-poll

show ping-poll

timeout (ping polling)

up-count

show counter ping-poll

Overview This command displays the counters for ping polling.

Syntax

```
show counter ping-poll [<1-100>]
```

Parameter	Description
<1-100>	A unique ping poll ID number. This displays the counters for the specified ping poll only. If you do not specify a ping poll, then this command displays counters for all ping polls.

Mode User Exec and Privileged Exec

Output Figure 31-1: 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 32: 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. This error can occur when your device does not have a route to the destination.
`CurrentUpCount`	The current number of sequential ping replies.
`CurrentFailCount`	The number of ping requests that have not received a ping reply in the current sample-size window.
`UpStateEntered`	Number of times the target device has entered the Up state.
`DownStateEntered`	Number of times the target device has entered the Down state.

Example To display counters for the polling instances, use the command:

```
awplus# show counter ping-poll
```

Related commands

debug ping-poll

ping-poll

show ping-poll

show ping-poll

Overview This command displays the settings and status of ping polls.

Syntax `show ping-poll [<1-100>|state {up|down}] [brief]`

Parameter	Description	
<1-100>	Displays settings and status for the specified polling instance.	
`state`	Displays polling instances based on whether the device they are polling is currently reachable or unreachable.	
	`up`	Displays polling instance where the device state is reachable.
	`down`	Displays polling instances where the device state is unreachable.
`brief`	Displays a summary of the state of ping polls, and the devices they are polling.	

Mode User Exec and Privileged Exec

Output Figure 31-2: 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 33: 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 ping-poll command.
Enabled	Whether the polling instance is enabled or disabled.

Table 33: 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 ip (ping-polling) command.	

Figure 31-3: 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 34: Parameters in output of the **show ping-poll** command

Parameter	Description	
Description	Optional description set for the polling instance with the description (ping-polling) command.	
Destination IP address	The IP address of the polled device, set with the ip (ping-polling) command.	
Status	The current status of the device being polled:	
	Up	The device is reachable.
	Down	The device is unreachable.
	Critical Up	The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down.
	Critical Down	The device is unreachable but the polling instance received a reply to the last ping packet, so the polled device may be coming back up.
Enabled	Whether the polling instance is enabled or disabled. The active (ping-polling) and active (ping-polling) commands enable and disable a polling instance.	
Source IP address	The source IP address sent in the ping packets. This is set using the source-ip 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 critical-interval command.	
Normal interval	The time period between pings when the device is reachable. This is set with the normal-interval command.	

Table 34: Parameters in output of the **show ping-poll** command (cont.)

Parameter	Description
`Fail count`	The number of pings that must be unanswered, within the total number of pings specified by the sample-size command, for the polling instance to consider the device unreachable. This is set using the fail-count 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 up-count 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 sample-size command.
`Length`	The number of data bytes to include in the data portion of the ping packet. This is set using the length (ping-poll data) command.
`Timeout`	The time in seconds that the polling instance waits for a response to a ping packet. This is set using the timeout (ping polling) command.
`Debugging`	Indicates whether ping polling debugging is **Enabled** or **Disabled**. This is set using the debug ping-poll command.

Examples

To display the ping poll settings and the status of all the polls, use the command:

```
awplus# show ping-poll
```

To display a summary of the ping poll settings, use the command:

```
awplus# show ping-poll brief
```

To display the settings for ping poll 6, use the command:

```
awplus# show ping-poll 6
```

To display a summary of the state of ping poll 6, use the command:

```
awplus# show ping-poll 6 brief
```

To display the settings of ping polls that have reachable devices, use the command:

```
awplus# show ping-poll state up
```

To display a summary of ping polls that have unreachable devices, use the command:

```
awplus# show ping-poll state down brief
```

Related commands

debug ping-poll

ping-poll

source-ip

Overview This command specifies the source IP address to use in ping packets.

By default, the polling instance uses the address of the interface through which it transmits the ping packets. It uses the device's local interface IP address when it is set. Otherwise, the IP address of the interface through which it transmits the ping packets is used.

The **no** variant of this command resets the source IP in the packets to the device's local interface IP address.

Syntax

```
source-ip {<ip-address>|<ipv6-address>}
no source-ip
```

Parameter	Description
<ip-address>	An IPv4 address in dotted decimal notation `A.B.C.D`
<ipv6-address>	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)

undebug ping-poll

Overview This command applies the functionality of the no debug ping-poll command.

Part 6: Virtual Private Networks (VPNs)

32 IPsec Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure Internet Protocol Security (IPsec) tunnel.

For introductory information about IPsec tunnel in AlliedWare Plus, including overview and configuration information, see the:

- Internet Protocol Security (IPsec) Feature Overview and_Configuration Guide

Command List

- "clear isakmp sa" on page 1076
- "crypto ipsec profile" on page 1077
- "crypto isakmp key" on page 1079
- "crypto isakmp peer" on page 1082
- "crypto isakmp profile" on page 1084
- "debug isakmp" on page 1086
- "dpd-interval" on page 1088
- "dpd-timeout" on page 1089
- "interface tunnel (IPsec)" on page 1090
- "lifetime (IPsec Profile)" on page 1091
- "lifetime (ISAKMP Profile)" on page 1092
- "no debug isakmp" on page 1093
- "pfs" on page 1094
- "rekey" on page 1096
- "show debugging isakmp" on page 1097
- "show interface tunnel (IPsec)" on page 1098
- "show ipsec counters" on page 1100

- "show ipsec peer" on page 1101
- "show ipsec policy" on page 1102
- "show ipsec profile" on page 1103
- "show ipsec sa" on page 1105
- "show isakmp counters" on page 1106
- "show isakmp key (IPsec)" on page 1107
- "show isakmp peer" on page 1108
- "show isakmp profile" on page 1109
- "show isakmp sa" on page 1111
- "show tunnel inline-processing counters" on page 1112
- "transform (IPsec Profile)" on page 1114
- "transform (ISAKMP Profile)" on page 1116
- "tunnel destination (IPsec)" on page 1118
- "tunnel inline-processing" on page 1120
- "tunnel local name (IPsec)" on page 1121
- "tunnel local selector" on page 1122
- "tunnel mode ipsec" on page 1124
- "tunnel oper-status-control" on page 1125
- "tunnel protection ipsec (IPsec)" on page 1128
- "tunnel remote name (IPsec)" on page 1129
- "tunnel remote selector" on page 1130
- "tunnel security-reprocessing" on page 1132
- "tunnel selector paired" on page 1133
- "tunnel source (IPsec)" on page 1134
- "undebug isakmp" on page 1136
- "version (ISAKMP)" on page 1137

clear isakmp sa

Overview Use this command to delete Internet Security Association Key Management Protocol (ISAKMP) Security Associations (SAs). SAs specify the Security Parameter Index (SPI), protocols, algorithms and keys for protecting a single flow of traffic between two IPSec peers. For more information about SA, see the Internet Protocol Security (IPSec) Feature Overview and Configuration Guide.

Syntax

```
clear [crypto] isakmp sa [peer <ipv4-addr>|<ipv6-addr>|
<hostname>] [force]
```

Parameter	Description
<ipv4-addr>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	Destination IPv6 address. The IPv4 address uses the format X:X::X:X.
<hostname>	Destination host name.
force	Force to clear ISAKMP SAs without negotiating with the peer.

Mode Privileged Exec

Examples To delete the ISAKMP security associations at the peer for an IPv6 address, use the command:

```
awplus# clear isakmp sa peer 2001:0db8::1
```

To delete the ISAKMP security associations at the peer for an IPv4 address, use the command:

```
awplus# clear isakmp sa peer 192.168.2.1
```

To delete the ISAKMP security associations at the peer for a host name, use the command:

```
awplus# clear isakmp sa peer remote.example.com
```

Related commands crypto isakmp key

show isakmp sa

Command Changes Version 5.4.7-0.1: Parameter <hostname> added for DDNS feature.

crypto ipsec profile

Overview Use this command to configure a custom IPsec profile.

An IPsec profile comprises one or more transforms that can be configured by using the transform (IPsec Profile) command.

Use the **no** variant to delete a previously created profile.

Syntax

```
crypto ipsec profile <profile_name>
no crypto ipsec profile <profile_name>
```

Parameter	Description
<profile_name>	Profile name. Profile names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Profile names can have only letters from a to z and A to Z, numbers from 0 to 9, - (dash), or _ (underscore).

Default The default IPsec profile with transforms in order of preference is listed in the following table. Which IPsec profile will actually be used depends on how the negotiation between the peers is carried out when establishing the connection. Note that you cannot delete or edit the default profile. Expiry time of 8 hours applies to the default IPsec profile.

Table 32-1: IPsec default profile

Attribute	Transform 1	Transform 2	Transform 3	Transform 4	Transform 5	Transform 6
Protocol	ESP	ESP	ESP	ESP	ESP	ESP
Encryption (all CBC)	AES256	AES256	AES128	AES128	3DES	3DES
Integrity (all HMAC)	SHA256	SHA1	SHA256	SHA1	SHA256	SHA1

Mode Global Configuration

Examples To configure a custom IPsec profile for establishing IPSec SAs with a remote peer, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# transform 2 protocol esp
integrity sha1 encryption 3des
```

To delete a custom profile, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto ipsec profile my_profile
```

Related commands

lifetime (IPsec Profile)

show ipsec profile

transform (IPsec Profile)

crypto isakmp key

Overview Use this command to configure an ISAKMP authentication key. These keys can be of type Pre-shared Key (PSK) or Extensible Authentication Protocol (EAP). Keys are stored encrypted in the running-configuration.

You must configure this key whenever you specify authentication keys in an (Internet Key Exchange) IKE policy and at both peers.

This command specifies both the value of the key and also an identifier (the hostname, address or policy parameters). This identifier is used to decide which key to use for a particular ISAKMP message exchange.

See the Usage section below for more information, and see the following guides for examples:

- Internet Protocol Security (IPsec) Feature Overview and_Configuration Guide
- GRE and Multipoint VPNs Feature Overview and Configuration Guide

Use the **no** variant to remove a key.

Syntax

```
crypto isakmp key [8] <key> hostname <hostname> [type {eap|psk}]
no crypto isakmp key [8] <key> hostname <hostname> [type {eap|psk}]
crypto isakmp key [8] <key> address {<ipv4-addr>|<ipv6-addr>} [type {eap|psk}]
no crypto isakmp key [8] <key> address {<ipv4-addr>|<ipv6-addr>} [type {eap|psk}]
crypto isakmp key [8] <key> policy <policy-name> [type {eap|psk}]
no crypto isakmp key [8] <key> policy <policy-name> [type {eap|psk}]
```

Parameter	Description
`crypto`	Security specific command.
`isakmp`	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
`key`	Pre-shared key (PSK) or Extensible Authentication Protocol (EAP).
<key>	Specify the key. Use any combination of alphanumeric characters up to 128 bytes.
`8`	Specifies that an encrypted key follows.
<hostname>	A hostname (e.g. example.com).
<ipv4-addr>	IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	IPv6 address. The IPv6 address uses the format X:X::X:X.

Parameter	Description
<policy-name>	The local policy name. This is the name of the tunnel (e.g. tunnel2).
`type`	ISAKMP key type
`eap`	Extensible Authentication Protocol. This can be used with multipoint VPN when performing RADIUS authentication. See the GRE and Multipoint VPNs Feature Overview and Configuration Guide for more information.
`psk`	Pre-shared Key (default)

Default ISAKMP keys do not exist.

Mode Global Configuration

Usage notes Use this command to configure an authentication key for use with the ISAKMP protocol.

Before a tunnel can be protected by IPsec, each endpoint of the tunnel must verify that they are communicating with an authorized entity. ISAKMP uses authentication keys in the initial handshake between peers to ensure both endpoints are allowed to communicate.

This command specifies both the value of the key and also an identifier which is used to decide which key to use for a particular ISAKMP message exchange. Because the responding endpoint does not identify itself to the local device until after the key is used, it is important that the key identifier is part of the tunnel configuration on the initiating device.

The tunnel configuration parameter used to select which key to use when negotiating IPsec protection for that tunnel is in priority order:

1) **tunnel remote name**

2) **tunnel destination <ipv4-address>|<ipv6-address>** (if the remote name is not specified)

3) **tunnel local name**

4) **tunnel source <ipv4-address>|<ipv6-address>** (if the remote name is not specified)

For point-to-point tunnels, we recommend you configure local and remote names on the tunnels. Then use the remote name of the other device to identify the authentication keys on the local device.

For point-to-multipoint tunnels, it may be necessary to identify the authentication key by the local name of the tunnel, if the ISAKMP negotiation is to be initiated by that tunnel. This is because it is not possible to configure multiple remote names. However, it is possible to use the expected remote addresses or names of the remote initiating tunnels to identify keys. This is because the remote tunnel will identify itself when it initiates a connection.

Examples

To configure a pre-shared authentication key of "friend", using a hostname, use the commands below:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend hostname
mypeer@my.domain.com
```

To remove that pre-shared key, use the commands below:

```
awplus# configure terminal
awplus(config)# no crypto isakmp key friend hostname
mypeer@my.domain.com
```

To configure a pre-shared already-encrypted authentication key, using an IPv4 address, use the commands below:

```
awplus# configure terminal
awplus(config)# crypto isakmp key 8 Nhe6ioQmzbysQaJr6Du+cA==
address 192.168.1.2
```

To configure a pre-shared key, using the local policy "tunnel2", use the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend policy tunnel2
```

To remove that key, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp key friend policy tunnel2
```

To configure an ISAKMP key using EAP, enter the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp key friend hostname example.com
type eap
```

Related commands

show isakmp key (IPsec)

tunnel destination (IPsec)

tunnel local name (IPsec)

tunnel remote name (IPsec)

Command changes

Version 5.4.9-0.1: **type** parameter added

Version 5.4.9-1.1: **policy** parameter added

crypto isakmp peer

Overview Use this command to configure a peer to use a specific ISAKMP profile.

Use the **no** variant to set the peer back to using the default profile.

Syntax

```
crypto isakmp peer address {<ipv4-addr>|<ipv6-addr>} profile
<profile-name>
no crypto isakmp peer address {<ipv4-addr>|<ipv6-addr>} profile
crypto isakmp peer dynamic profile <profile-name>
no crypto isakmp peer dynamic profile
crypto isakmp peer hostname <hostname> profile <profile-name>
no crypto isakmp peer hostname <hostname> profile
crypto isakmp peer policy <policy-name> profile <profile-name>
no crypto isakmp peer policy <policy-name> profile
```

Parameter	Description
<ipv4-addr>	IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	IPv6 address. The IPv6 address uses the format X:X::X:X.
dynamic	Remote endpoint with a dynamic IP address.
<hostname>	Remote endpoint with a host name as the destination.
<policy-name>	The name of a local policy. This is the name of the tunnel (e.g. tunnel2).
<profile-name>	Profile name.

Default By default, all peers use the default profile.

Mode Global Configuration

Usage notes Use this command to configure a peer to use a specific ISAKMP profile.

When IPsec protection is applied to a tunnel, an ISAKMP profile is selected for use when IPsec parameters need to be negotiated. This profile is chosen when the tunnel first becomes active, and so must be selected based on local configuration only.

The tunnel configuration parameter used to select which ISAKMP profile to use when negotiating IPsec protection for that tunnel is in the following priority order:

1) **tunnel destination dynamic** (if a dynamic profile has been configured)

2) **tunnel endpoint dynamic** (if a dynamic profile has been configured)

3) **tunnel remote name**

4) **tunnel destination <ipv4-address>|<ipv6-address>** (if the remote name is not specified)

5) **tunnel endpoint <ipv4-address>**

6) **tunnel local name**

7) **tunnel source <ipv4-address>|<ipv6-address>** (if the remote name is not specified)

8) **tunnel destination <hostname>** (if the hostname is not specified)

9) **tunnel endpoint <hostname>** (if the hostname is not specified)

Examples To configure a profile for a peer, using a dynamic IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp peer dynamic profile peer_profile
```

To set the profile for the peer back to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp peer dynamic profile
```

To configure a profile for a peer, using a local policy name of "tunnel2", use the commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp peer policy tunnel2 profile
peer-profile
```

To set the profile for the peer back to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp peer policy tunnel2 profile
```

Related commands

show isakmp peer

tunnel destination (IPsec)

tunnel local name (IPsec)

tunnel source (IPsec)

tunnel remote name (IPsec)

Command Changes

Version 5.4.7-0.1: **hostname** parameter added.

Version 5.4.9-1.1: **policy** parameter added.

crypto isakmp profile

Overview Use this command to configure a custom ISAKMP profile.

An ISAKMP profile comprises one or more transforms that can be configured by using the transform (ISAKMP Profile) command.

Use the **no** variant to delete a previously created profile.

Syntax

```
crypto isakmp profile <profile_name>
no crypto isakmp profile <profile_name>
```

Parameter	Description
<profile_name>	Profile name. Profile names are case insensitive and can be up to 64 characters long composed of printable ASCII characters. Profile names can have only letters from a to z and A to Z, numbers from 0 to 9, - (dash), or _ (underscore).

Default Which ISAKMP profile transform will actually be used depends on how the negotiation between the peers is carried out when establishing the connection. For more information about default ISAKMP profiles, see the following table. Note that you cannot delete or edit the default profile. Expiry time of 24 hours applies to the default profile.

Table 32-2: ISAKMP default profile

Attribute	Encryption	Integrity	Group	Authentication
Transform 1	AES256	SHA256	14	Pre-shared
Transform 2	AES256	SHA256	16	Pre-shared
Transform 3	AES256	SHA1	14	Pre-shared
Transform 4	AES256	SHA1	16	Pre-shared
Transform 5	AES128	SHA256	14	Pre-shared
Transform 6	AES128	SHA256	16	Pre-shared
Transform 7	AES128	SHA1	14	Pre-shared
Transform 8	AES128	SHA1	16	Pre-shared
Transform 9	3DES	SHA256	14	Pre-shared
Transform 10	3DES	SHA256	16	Pre-shared
Transform 11	3DES	SHA1	14	Pre-shared
Transform 12	3DES	SHA1	16	Pre-shared

Mode Global Configuration

Examples

To configure a custom ISAKMP profile for establishing ISAKMP SAs with a remote peer, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# transform 2 integrity sha1
encryption 3des group 5
```

To delete a custom profile, use the following commands:

```
awplus# configure terminal
awplus(config)# no crypto isakmp profile my_profile
```

Related commands

dpd-interval

dpd-timeout

lifetime (ISAKMP Profile)

transform (ISAKMP Profile)

version (ISAKMP)

Validation Commands

show isakmp profile

debug isakmp

Overview Use this command to enable debugging ISAKMP.

To disable debugging ISAKMP, see no debug isakmp or undebug isakmp.

Syntax `debug [crypto] isakmp [info|trace|all]`

Parameter	Description
`debug`	Debugging function.
`crypto`	Security specific command.
`isakmp`	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
`info`	Informational debug messages such as protocol events.
`trace`	Verbose debug messages including protocol events and message traces.
`all`	All debug enabled.

Mode Privileged Exec

Examples Figure 32-1: Example output from the **debug isakmp** command on the console.

```
awplus#debug isakmp info
awplus#terminal monitor
% Warning: Console logging enabled
awplus#show ipsec peer
21:03:42 awplus IMISH[30349]: show ipsec peer


10.2.0.10
  IPSEC
    Selector: 0.0.0.0/0 0.0.0.0/0   tunnel1
    Profile: default
  ISAKMP
    LocalID: 10.1.0.10
    RemoteID: 10.2.0.10
awplus#ping 192.168.1.2

PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
21:04:13 awplus iked: [DEBUG]: ike_pfkey.c:622:sadb_acquire_callback():
sadb_acquire_callback: seq=6 reqid=409
6 satype=96 sa_src=10.1.0.10[0] sa_dst=10.2.0.10[0] samode=229 selid=1
21:04:13 awplus iked: [DEBUG]: isakmp.c:918:isakmp_initiate(): new request (seq:6
spid:1 reqid:4096)
21:04:13 awplus iked: [DEBUG]: ikev2.c:758:ikev2_initiate(): creating new ike_sa
21:04:13 awplus iked: [DEBUG]: ike_sa.c:431:ikev2_allocate_sa():
ikev2_create_sa((nil), 10.1.0.10[500], 10.2.0
.10[500], 0x810b678)
21:04:13 awplus iked: [DEBUG]: ike_sa.c:434:ikev2_allocate_sa(): sa: 0x810d3a0
21:04:13 awplus iked: [DEBUG]: ikev2.c:800:ikev2_initiate(): child_sa: 0x810dd60
21:04:13 awplus iked: [DEBUG]: ikev2_child.c:139:ikev2_child_state_set(): child_sa
0x810dd60 state IDLING -> G
ETSPI
21:04:13 awplus iked: [DEBUG]: ike_pfkey.c:269:sadb_getspi(): sadb_getspi: seq=6,
satype=96
21:04:13 awplus iked: [DEBUG]: ike_pfkey.c:622:sadb_acquire_callback():
sadb_acquire_callback: seq=7 reqid=409
6 satype=96 sa_src=10.1.0.10[0] sa_dst=10.2.0.10[0] samode=229 selid=1
21:04:13 awplus iked: [DEBUG]: isakmp.c:918:isakmp_initiate(): new request (seq:7
spid:1 reqid:4096)
21:04:13 awplus iked: [DEBUG]: ikev2.c:800:ikev2_initiate(): child_sa: 0x810ec68
21:04:13 awplus iked: [DEBUG]: ikev2_child.c:139:ikev2_child_state_set(): child_sa
0x810ec68 state IDLING -> G
ETSPI

awplus#no debug isakmp
awplus#show debugging isakmp

ISAKMP Debugging status:
  ISAKMP Informational debugging is disabled
  ISAKMP Trace debugging is disabled
```

Related commands no debug isakmp

undebug isakmp

dpd-interval

Overview Use this command to specify the Dead Peer Detection (DPD) interval for an ISAKMP profile.

DPD is an IKE mechanism using a form of keep-alive to determine if a tunnel peer is still active.

The interval parameter specifies the amount of time the device waits for traffic from its peer before sending a DPD acknowledgment message.

Use the **no** variant to set the interval to its default (30 seconds).

Syntax

```
dpd-interval <10-86400>
no dpd-interval
```

Parameter	Description
<10-86400>	Interval expressed in seconds.

Default If you do not specify an interval, the default interval of 30 seconds applies.

Mode ISAKMP Profile Configuration

Examples To specify a DPD interval, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# dpd-interval 20
```

To set the interval to its default, use the following commands:

```
awplus(config-isakmp-profile)# no dpd-interval
```

Related commands crypto isakmp profile

Validation Commands show isakmp profile

dpd-timeout

Overview Use this command to specify a Dead Peer Detection (DPD) timeout for IKEv1.

DPD is an IKE mechanism using a form of keep-alive to determine if a tunnel peer is still active.

DPD timeout defines the timeout interval after which all connections to a peer are deleted in case of inactivity. This only applies to IKEv1, in IKEv2 the default retransmission timeout applies as every exchange is used to detect dead peers.

Use the **no** variant to set the timeout to its default (150 seconds).

Syntax

```
dpd-timeout <10-86400>
no dpd-timeout
```

Parameter	Description
<10-86400>	Timeout in seconds.

Default If you do not specify a timeout, the default timeout of 150 seconds applies.

Mode ISAKMP Profile Configuration

Examples To specify a DPD timeout for IKEv1, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile
awplus(config-isakmp-profile)# dpd-timeout 200
```

To set the timeout to its default, use the following command:

```
awplus(config-isakmp-profile)# no dpd-timeout
```

Related commands crypto isakmp profile

Related commands show isakmp profile

interface tunnel (IPsec)

Overview Use this command to create a tunnel interface or to enter Interface mode to configure an existing tunnel. Tunnel interfaces are identified by an index identifier that is an integer in the range from 0 through 65535.

Use the **no** variant of this command to remove a previously created tunnel interface.

Syntax

```
interface tunnel<0-65535>
no interface tunnel<tunnel-index>
```

Parameter	Description
<0-65535>	Specify a tunnel interface index identifier in the range from 0 to 65535.

Default Tunnel interfaces do not exist.

Mode Global Configuration

Usage notes After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

Note that you need to designate a tunnel mode, tunnel source address, tunnel destination address, IP address of tunnel interface and use tunnel protection ipsec (IPsec) command to encrypt and authenticate the packets travelling though the tunnel.

Examples To configure an IPsec tunnel interface with index 100, enter the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel100
awplus(config-if)# tunnel mode ipsec ipv4
```

To remove the IPsec tunnel interface tunnel100, enter the commands below:

```
awplus# configure terminal
awplus(config)# no interface tunnel100
```

Command changes Version 5.4.7-2.1: increased range for **tunnel** index identifier.

lifetime (IPsec Profile)

Overview Use this command to specify a lifetime for an IPsec SA.

Lifetime measures how long the IPsec SA can be maintained before it expires. Lifetime prevents a connection from being used too long.

Use the **no** variant to set the lifetime to default (28800 seconds).

Syntax

```
lifetime seconds <300-31449600>
no lifetime seconds
```

Parameter	Description
<300-31449600>	Lifetime in seconds.

Default If you do not specify a lifetime, the default lifetime of 28800 seconds (8 hours) applies.

Mode IPsec Profile Configuration

Examples To specify a lifetime for an IPsec SA, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# lifetime seconds 400
```

To set the lifetime to its default, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# no lifetime seconds
```

Related commands crypto ipsec profile

lifetime (ISAKMP Profile)

Overview Use this command to specify a lifetime for an ISAKMP SA.

Lifetime measures how long the ISAKMP SA can be maintained before it expires. Lifetime prevents a connection from being used too long.

Use the **no** variant to set the lifetime to default (86400 seconds).

Syntax

```
lifetime <600-31449600>
no lifetime
```

Parameter	Description
<600-31449600>	Lifetime in seconds.

Default If you do not specify a lifetime, the default lifetime of 86400 seconds (8 hours) applies.

Mode ISAKMP Profile Configuration

Examples To specify a lifetime for an ISAKMP SA, use the following commands:

```
awplus(config)# configure isakmp profile my_profile
awplus(config-isakmp-profile)# lifetime 700
```

To set the lifetime to its default, use the following commands:

```
awplus(config-isakmp-profile)# no lifetime
```

Related commands crypto isakmp profile

no debug isakmp

Overview Use this command to disable debugging ISAKMP.

To enable debugging ISAKMP, see debug isakmp.

Syntax

```
no [crypto] isakmp [info|trace|all]
```

Parameter	Description
`no`	Disable debugging function.
`crypto`	Security specific.
`isakmp`	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
`info`	Informational debug messages such as protocol events.
`trace`	Verbose debug messages including protocol events and message traces.
`all`	All debug enabled.

Mode Privileged Exec

Related commands debug isakmp

undebug isakmp

pfs

Overview Use this command to enable PFS and set a Diffie-Hellman group for PFS in an IPsec profile.

Use the **no** variant to disable PFS.

Syntax

```
pfs {2|5|14|15|16|18}
no pfs
```

Parameter	Description
2	1024-bit MODP Group
5	1536-bit MODP Group
14	2048-bit MODP Group
15	3072-bit MODP Group
16	4096-bit MODP Group
18	8192-bit MODP Group

Default PFS is disabled.

Mode IPsec Profile Configuration

Usage notes Perfect Forward Secrecy (PFS) ensures generated keys, for example IPsec SA keys are not compromised if any other keys, for example, ISAKMP SA keys are compromised.

The specified PFS group must match the PFS group setting on the peer - especially when IKEv2 is used for ISAKMP SA negotiation. With IKEv2, if there is a PFS group mismatch an IPsec SA will be established and the tunnel will come up because PFS is not required for the initial child SA negotiation. However, when the IPsec SA rekeys it will fail due to the PFS group mismatch, and upon IPsec SA expiry the tunnel will no longer be able to carry traffic.

Examples To enable PFS and set a Diffie-Hellman group for PFS, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
awplus(config-ipsec-profile)# pfs 15
```

To disable PFS, use the following command:

```
awplus(config-ipsec-profile)# no pfs
```

Related commands crypto ipsec profile

Validation Commands show ipsec profile

rekey

Overview Use this command to set the rekey policy for an IPsec profile. This policy will be used to make a decision or whether the SA will rekey at its expiry.

The options are **always**, **never**, and **on-demand**. The **on-demand** option makes its decision based on whether the link has seen any traffic since the SA's last rekey.

Use the **no** variant of this command to set the rekey policy back to its default of **always**.

Syntax

```
rekey {always|never|on-demand}
no rekey
```

Parameter	Description
`always`	Always rekey this SA (default)
`never`	Never rekey this SA
`on-demand`	Only rekey this SA if it has been used since the last rekey

Default By default, an IPsec SA will always rekey.

Mode IPsec Profile Configuration

Usage notes These options may be useful if you have a hub and spoke VPN topology and need to provision more than the maximum number of concurrent active VPNs supported by your device. **Never** and **on-demand** allow unused VPNs to be aged out, making more efficient use of the number of available VPNs.

Example To only rekey when traffic is detected over the interface, for the profile named 'myprofile', use the commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile myprofile
awplus(config-ipsec-profile)# rekey on-demand
```

To reset the rekey policy back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# crypto ipsec profile myprofile
awplus(config-ipsec-profile)# no rekey
```

Related commands

crypto ipsec profile

show ipsec profile

Command changes Version 5.4.9-2.1: command added

show debugging isakmp

Overview Use this command to show if debugging ISAKMP is enabled.

Syntax

```
show debugging [crypto] isakmp
```

Parameter	Description
`debugging`	Debugging information.
`crypto`	Security specific command.
`isakmp`	Internet Security Association Key Management Protocol provides a common framework for key management implementations.

Mode Privileged Exec

Examples To show if debugging ISAKMP is enabled, enter the command below:

```
awplus# show debugging isakmp
```

Output Figure 32-2: Example output from the **show debugging isakmp** command

```
awplus#show debugging isakmp
ISAKMP Debugging status:
  ISAKMP Informational debugging is enabled
  ISAKMP Trace debugging is disabled
```

show interface tunnel (IPsec)

Overview Use this command to display status information of tunnels.

The tunnel remains inactive if no valid tunnel source or tunnel destination is configured.

Syntax `show interface tunnel<tunnel-index>`

Parameter	Description
`tunnel`	Specify this parameter to display tunnel status information of a given tunnel identified by the <*tunnel-index*> parameter.
`<tunnel-index>`	Specify a tunnel index in the range from 0 through 65535.

Mode Privileged Exec

Examples To display status information for IPsec tunnel 'tunnel2', use the command:

```
awplus# show interface tunnel2
```

Output Figure 32-3: Example output from the **show interface tunnel** command

```
awplus#show interface tunnel2
Interface tunnel2
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 192.168.1.2/30
  index 23 metric 1 mtu 1438
  <UP,RUNNING,MULTICAST>
  VRF Binding: Not bound
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Tunnel source eth1 (200.1.45.1), destination 200.1.15.1
  Tunnel name local 200.1.45.1, remote 200.1.15.1
  Tunnel traffic selectors (ID, local, remote)
    1    0.0.0.0/0                  0.0.0.0/0
  Tunnel protocol/transport ipsec ipv4, key disabled, sequencing disabled
  Checksumming of packets disabled, DF bit set, path MTU discovery disabled
  Tunnel protection via IPsec (profile "default")
  Tunnel inline-processing enabled
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0, broadcast packets 0
    input average rate : 30 seconds 0 bps, 5 minutes 0 bps
    output average rate: 30 seconds 0 bps, 5 minutes 0 bps
  Time since last state change: 0 days 00:00:07
```

Related commands interface tunnel (IPsec)

show ipsec counters

Overview Use this command to show IPSec counters.

Syntax

```
show [crypto] ipsec counters
```

Parameter	Description
`crypto`	Security specific command.
`ipsec`	Internet Protocol Security defines the protection of IP packets using encryption and authentication.
`counters`	Show IPSec transformation statistic.

Mode Privileged Exec

Examples To show IPSec counters, enter the command below:

```
awplus# show ipsec counters
```

Output Figure 32-4: Example output from the **show ipsec counters** command

```
awplus#show ipsec counters
Name                          Value
-------------------------------------
InError                       0
InBufferError                 0
InHdrError                    0
InNoStates                    0
InStateProtoError             0
InStateModeError              0
InStateSeqError               0
InStateExpired                0
InStateMismatch               0
InStateInvalid                0
InTmplMismatch                0
InNoPols                      0
InPolBlock                    0
InPolError                    0
OutError                      0
OutBundleGenError             0
OutBundleCheckError           0
OutNoStates                   0
OutStateProtoError            0
OutStateModeError             0
OutStateSeqError              0
OutStateExpired               0
OutPolBlock                   0
OutPolDead                    0
OutPolError                   0
FwdHdrError                   0
```

show ipsec peer

Overview Use this command to show IPSec information on a per peer basis.

Syntax `show [crypto] ipsec peer [<hostname>|<ipv4-addr>|<ipv6-addr>]`

Parameter	Description
`crypto`	Security specific command.
`peer`	Remote endpoint.
<hostname>	Destination hostname.
<ipv4-addr>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	Destination IPv6 address. The IPv6 address uses the format X:X::X:X.

Mode Privileged Exec

Examples To show IPSec information on a per peer basis, enter the command below:

```
awplus# show ipsec peer 172.16.0.1
```

Output Figure 32-5: Example output from the **show ipsec peer** command

```
awplus#show ipsec peer 172.16.0.1
172.16.0.2
  IPsec
    Selectors (local:remote)
      Address:  0.0.0.0/0 : 0.0.0.0/0
      Protocol: any:any
      Port:     any:any
      Mark:     1:1
    Profile: default
    SAs:
      SPI (In:Out): ca865389:c9c7e3d3
        Selectors:  192.168.1.0/24 : 192.168.2.0/24
        Proto:      ESP
        Mode:       tunnel
        Encryption: AES256
        Integrity:  SHA256
        Expires:    28796s
  ISAKMP
    LocalID:  172.16.0.1
    RemoteID: 172.16.0.2
    SAs:
      Cookies (Initiator:Responder) 03071749781e5992:93f8457816d3d40d
        Ver:            2           Lifetime: 84569s    State: Established
        Authentication: PSK         Group:    14
        Encryption:     AES256      NATT:     no
        Integrity:      SHA256      DPD:      yes
```

show ipsec policy

Overview Use this command to show IPSec policies.

Syntax

```
show [crypto] ipsec policy
```

Parameter	Description
`crypto`	Security specific command.
`ipsec`	Internet Protocol Security defines the protection of IP packets using encryption and authentication.
`policy`	Policy.

Mode Privileged Exec

Examples To show IPSec policies, enter the command below:

```
awplus# show ipsec policy
```

Output Figure 32-6: Example output from the **show ipsec policy** command

```
awplus#show ipsec policy
Traffic Selector (addresses protocol ports interface)
  Profile           Peer
0.0.0.0/0 0.0.0.0/0   tunnel1
  default           10.2.0.10
```

show ipsec profile

Overview Use this command to show IPsec default and custom profiles.

An IPsec profile consists of a set of parameters that are used by IPsec when establishing IPsec SAs with a remote peer. AlliedWare Plus provides default ISAKMP and IPsec profiles that contain a priority ordered set of transforms that are considered secure by the security community.

Syntax `show [crypto] ipsec profile [<profile_name>]`

Parameter	Description
`crypto`	Security specific.
`ipsec`	Internet Protocol Security defines the protection of IP packets using encryption and authentication.
`profile`	An IPsec profile consists of a set of parameters that are used by IPsec SAs with a remote peer.
<profile_name>	Custom profile name.

Mode Privileged Exec

Examples To show all IPsec profiles, including the default profile, use the following command:

```
awplus# show ipsec profile
```

Output Figure 32-7: Example output from the **show ipsec profile** command

```
awplus#show ipsec profile
IPsec Profile: default
  Replay-window: 32
  Rekey: Always
  Expiry: 8h
  PFS group: disabled
  Transforms:
  Protocol Integrity Encryption
    1 ESP SHA256 AES256
    2 ESP SHA1 AES256
    3 ESP SHA256 AES128
    4 ESP SHA1 AES128
    5 ESP SHA256 3DES
    6 ESP SHA1 3DES

IPsec Profile: my_profile
 Replay-window: 32
 Rekey: On Demand
 Expiry: 8h
 PFS group: disabled
 Transforms:
 Protocol Integrity Encryption
  2 ESP SHA1 3DES
```

Examples To show IPsec profile “my_profile”, use the command:

```
awplus# show ipsec profile my_profile
```

Output Figure 32-8: Example output from the **show ipsec profile** command

```
awplus#show ipsec profile my_profile
IPsec Profile: my_profile
  Replay-window: 32
  Rekey: On Demand
  Expiry: 8h
  PFS group: disabled
  Transforms:
  Protocol Integrity Encryption
   2 ESP SHA1 3DES
```

Related commands crypto ipsec profile

show ipsec sa

Overview Use this command to view the settings used by current security associations. SAs specify the Security Parameter Index (SPI), protocols, algorithms and keys for protecting a single flow of traffic between two IPSec peers. For more information about SA, see the Internet Protocol Security (IPSec) Feature Overview and Configuration Guide.

Syntax

```
show [crypto] ipsec sa
```

Parameter	Description
`crypto`	Security specific command.
`ipsec`	Internet Protocol Security defines the protection of IP packets using encryption and authentication.
`sa`	Security Association.

Mode Privileged Exec

Examples To view the settings used by current security associations, enter the command below:

```
awplus# show ipsec sa
```

Output Figure 32-9: Example output from the **show ipsec sa** command

```
awplus#show ipsec sa
------------------------------------------------------------------------
Peer                SPI (in:out)          Mode          Proto  Expires
                    Encryption            Integrity     PFS
------------------------------------------------------------------------
10.0.0.20           c2d8c150:7b24d3f5     tunnel        ESP    28786s
                    AES256                SHA256        -
10.0.0.22           c6c2ad0d:0d008e3d     tunnel        ESP    3582s
                    3DES                  SHA1          -
10.0.0.25           cb36f9dd:cd87a834     tunnel        ESP    28778s
                    AES128                SHA1          2
```

show isakmp counters

Overview Use this command to show ISAKMP counters.

Syntax

```
show [crypto] isakmp counters
```

Parameter	Description
`crypto`	Security specific command.
`isakmp`	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
`counters`	Show ISAKMP counters.

Mode Privileged Exec

Examples To show ISAKMP counters, enter the command below:

```
awplus# show isakmp counters
```

Output Figure 32-10: Example output from the **show isakmp counters** command

```
awplus#show isakmp counters
Name                          Value
-------------------------------------
ikeInitRekey                  0
ikeRspRekey                   0
ikeChildSaRekey               0
ikeInInvalid                  0
ikeInInvalidSpi               0
ikeInInitReq                  0
ikeInInitRsp                  0
ikeOutInitReq                 0
ikeOutInitRsp                 0
ikeInAuthReq                  0
ikeInAuthRsp                  0
ikeOutAuthReq                 0
ikeOutAuthRsp                 0
ikeInCrChildReq               0
ikeInCrChildRsp               0
ikeOutCrChildReq              0
ikeOutCrChildRsp              0
ikeInInfoReq                  0
ikeInInfoRsp                  0
ikeOutInfoReq                 0
ikeOutInfoRsp                 0
```

show isakmp key (IPsec)

Overview Use this command to show ISAKMP authentication keys. These keys can be of type Pre-shared Key (PSK) or Extensible Authentication Protocol (EAP). Keys are stored encrypted in the running-configuration.

Syntax

```
show [crypto] isakmp key
```

Parameter	Description
`crypto`	Security specific command.
`isakmp`	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
`key`	Pre-shared key (PSK), or Extensible Authentication Protocol (EAP).

Mode Privileged Exec

Examples To show the ISAKMP keys, enter the command below:

```
awplus# show isakmp key
```

Output Figure 32-11: Example output from the **show isakmp key** command

```
awplus#show isakmp key
Hostname/IP address          PSK               EAP
-------------------------------------------------------------------
10.1.1.1                   mykeyone          mykeytwo
10.1.5.1                   mykeyfive         -
10.1.7.1                   -                 mykeyseven
```

Related commands crypto isakmp key

show isakmp peer

Overview Use this command to show ISAKMP profile and key status for ISAKMP peers.

Syntax

```
show isakmp peer [<hostname>|<ipv4-addr>|<ipv6-addr>]
```

Parameter	Description
<hostname>	Destination hostname.
<ipv4-addr>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-addr>	Destination IPv6 address. The IPv6 address uses the format X:X::X:X.

Mode Privileged Exec

Examples To show ISAKMP profile and key status for ISAKMP peers, use the following command:

```
awplus# show isakmp peer
```

Output Figure 32-12: Example output from the **show isakmp peer** command

```
awplus#show isakmp peer
Peer                    Profile (* incomplete)           Key
-------------------------------------------------------------------
10.1.1.1                default                          PSK, EAP
10.1.5.1                SECURE                           PSK
example.com             LEGACY                           EAP
```

Related commands crypto isakmp peer

Command changes Version 5.4.7-0.1: Parameter **hostname** added for DDNS feature.

show isakmp profile

Overview Use this command to show ISAKMP default and custom profiles.

Syntax

```
show [crypto] isakmp profile [<profile_name>]
```

Parameter	Description
<profile_name>	Custom profile name.

Mode Privileged Exec

Examples To show ISAKMP profiles, including the default profile, use the command:

```
awplus# show isakmp profile
```

Output Figure 32-13: Example output from the **show isakmp profile** command

```
awplus#show isakmp profile
ISAKMP Profile: default
  Version:        IKEv2
  Authentication: PSK
  Expiry:         24h
  DPD Interval:   30s
  Transforms:
       Integrity   Encryption  DH Group
    1    SHA256      AES256      14
    2    SHA256      AES256      16
    3    SHA1        AES256      14
    4    SHA1        AES256      16
    5    SHA256      AES128      14
    6    SHA256      AES128      16
    7    SHA1        AES128      14
    8    SHA1        AES128      16
    9    SHA256      3DES        14
   10    SHA256      3DES        16
   11    SHA1        3DES        14
   12    SHA1        3DES        16

ISAKMP Profile: my_profile
  Version:        IKEv2
  Authentication: PSK
  Expiry:         24h
  DPD Interval:   30s
  Transforms:
       Integrity   Encryption  DH Group
    2    SHA1        3DES         5
```

Examples To show ISAKMP profile “my_profile”, use the command:

```
awplus# show isakmp profile my_profile
```

Output Figure 32-14: Example output from the **show isakmp profile** command

```
awplus#show isakmp profile my_profile
ISAKMP Profile: my_profile
  Version:        IKEv2
  Authentication: PSK
  Expiry:         24h
  DPD Interval:   30s
  Transforms:
       Integrity   Encryption  DH Group
    2    SHA1         3DES         5
```

Related commands crypto isakmp profile

show isakmp sa

Overview Use this command to show current IKE security associations at a peer.

Syntax

```
show [crypto] isakmp sa
```

Parameter	Description
`crypto`	Security specific command.
`isakmp`	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
`sa`	Security Association.

Mode Privileged Exec

Examples To show current IKE security associations at a peer, enter the command below:

```
awplus# show isakmp sa
```

Output Figure 32-15: Example output from the **show isakmp sa** command

```
awplus#show isakmp sa
-------------------------------------------------------------------------------
Peer                Cookies (initiator:responder)       Auth  Ver   Expires
                    Encryption    Integrity    Group    DPD   NATT  State
-------------------------------------------------------------------------------
10.0.0.20           f93c2717a1ece407:972bc0c77344d7a4   PSK   1     78340s
                    AES256        SHA256       2        yes   no    Established
10.0.0.22           ccb7f90b54945375:2642525bd20f3428   PSK   1     3334s
                    3DES          SHA1         2        yes   no    Established
10.0.0.25           bd0efef134c86656:d46d0b1b72b46444   PSK   1     819s
                    AES128        SHA1         2        yes   no    Established
```

show tunnel inline-processing counters

Overview Use this command to show the tunnel inline-processing counters.

Syntax

```
show tunnel inline-processing counters
```

Mode Privileged Exec

Usage notes Global counters show packet counts (esp, frames, nsh, oam), packet decisions (decrypts, drops), and IPsec SAs tracked by tunnel inline (msg_...,sa_added, sa_deleted).

Per worker counters show the packet counts and decisions made by each worker and activity counters (fetch, sleep, wakeup,...).

Example To display tunnel inline-processing counters, use the command:

```
awplus# show tunnel inline-processing counters
```

Output Figure 32-16: Example output from **show tunnel inline-processing counters**

```
show tunnel inline-processing counters
Global Counters:
                decrypts                  4913089
                    drop                        0
            err_not_esp                         0
         err_trans_auth                         0
       err_trans_crypto                         0
                    esp                   4913089
     esp_error_internal                         0
  esp_error_invalid_hmac                        0
    esp_error_malformed                         0
   esp_error_replay_fail                        0
             esp_no_sa                          0
              espinudp                          0
                frames                    7518246
                ignore                    2605157
            msg_del_sa                          0
         msg_expired_sa                         0
           msg_flush_sa                         0
            msg_new_sa                          0
           msg_unknown                          0
         msg_updated_sa                         0
                   nsh                    7518246
                   oam                          0
             sa_added                           2
            sa_deleted                          0...
```

```
worker0: sleeping
              decrypts                    1386914
                  drop                          0
                   esp                    1386914
      esp_error_internal                         0
  esp_error_invalid_hmac                         0
     esp_error_malformed                         0
   esp_error_replay_fail                         0
              esp_no_sa                          0
               espinudp                          0
                fetch00                     617322
                fetch01                     407403
             fetch02_03                     155630
             fetch04_07                      36150
             fetch08_15                      11152
             fetch16_31                       2457
             fetch32_63                       2553
               fetch64_                       2787
                 frames                    2669292
                 ignore                    1282378
                    nsh                    2669292
                    oam                          0
              return00                           0
              return01                      407403
            return02_03                     155630
            return04_07                      36150
            return08_15                      11152
            return16_31                       2457
            return32_63                       2553
              return64_                       2787
                  sleep                     617322
              sleep_cmd                     617322
             sleep_user                          0
             sleep_work                     617322
                 wakeup                     617321
            wakeup_cmd                           0
           wakeup_user                           0
           wakeup_work                     617321
```

Related commands tunnel inline-processing

Command changes Version 5.5.2-1.1: command added

transform (IPsec Profile)

Overview Use this command to create an IPsec profile transform, which specifies the encryption and authentication algorithms used to protect data.

Use the **no** variant to delete a previously created transform.

Syntax

```
transform <1-255> protocol esp integrity {sha1|sha256|sha512}
encryption {3des|aes128|aes192|aes256|null}
```

```
transform <1-255> protocol esp integrity {gcm8|gcm12|gcm16}
encryption {aes128|aes192|aes256}
```

```
no transform <1-255>
```

Parameter	Description
<1-255>	Transform priority (1 is the highest).
sha1	Secure Hash Standard with 160-bit digest size.
sha256	Secure Hash Standard with 256-bit digest size.
sha512	Secure Hash Standard with 512 bit digest size.
3des	Triple DES symmetric key block cipher with a 168-bit key.
aes128	Advanced Encryption Standard symmetric key block cipher with a 128-bit key.
aes192	Advanced Encryption Standard symmetric key block cipher with a 192-bit key.
aes256	Advanced Encryption Standard symmetric key block cipher with a 256-bit key.
gcm8	Galois/Counter Mode that uses an 8-byte authentication tag.
gcm12	Galois/Counter Mode that uses a 12 byte authentication tag.
gcm16	Galois/Counter Mode that uses a 16 byte authentication tag.
null	No encryption. This option is not intended for use in a live network. It should only be used for testing purposes.

Default By default, an IPsec profile has no transforms and so will not be active.

Mode IPsec Profile Configuration

Examples To configure an IPsec profile transform, use the following commands:

```
awplus(config)# crypto ipsec profile my_profile
```

```
awplus(config-ipsec-profile)# transform 2 protocol esp
integrity sha1 encryption 3des
```

To delete a created transform, use the following command:

```
awplus(config-ipsec-profile)# no transform 2
```

Related commands crypto ipsec profile

Validation Commands show ipsec profile

Command changes Version 5.5.3-2.1: **gcm** parameters added

transform (ISAKMP Profile)

Overview Use this command to create an ISAKMP profile transform which specifies the encryption and authentication algorithms used to protect data in the tunnel.

Use the **no** variant to delete a previously created transform.

Syntax

```
transform <1-255> integrity {sha1|sha256|sha512} encryption
{3des|aes128|aes192|aes256} group {2|5|14|15|16|18}
```

```
no transform <1-255>
```

Parameter	Description
<1-255>	Transform priority (1 is the highest)
sha1	Secure Hash Standard with 160-bit digest size
sha256	Secure Hash Standard with 256-bit digest size
sha512	Secure Hash Standard with 512 bit digest size
3des	Triple DES symmetric key block cipher with a 168-bit key
aes128	Advanced Encryption Standard symmetric key block cipher with a 128-bit key
aes192	Advanced Encryption Standard symmetric key block cipher with a 192-bit key
aes256	Advanced Encryption Standard symmetric key block cipher with a 256-bit key
group	Diffie-Hellman group
2	1024-bit MODP Group
5	1536-bit MODP Group
14	2048-bit MODP Group
15	3072-bit MODP Group
16	4096-bit MODP Group
18	8192-bit MODP Group

Default By default, an ISASMP profile has no transforms and so will not be active.

Mode ISAKMP Profile Configuration

Examples To create an ISAKMP profile transform, use the following commands:

```
awplus(config)# crypto isakmp profile my_profile
```

```
awplus(config-isakmp-profile)# transform 2 integrity sha1
encryption 3des group 5
```

To delete a created transform, use the following command:

```
awplus(config-isakmp-profile)# no transform 2
```

Related commands crypto isakmp profile

tunnel destination (IPsec)

Overview Use this command to specify a destination IPv4 or IPv6 address or destination network name for the remote end of the tunnel.

Use the **no** variant of this command to remove a configured tunnel destination address.

Syntax

```
tunnel destination {<WORD>|<ipv4-address>|<ipv6-address>}
no tunnel destination {<WORD>|<ipv4-address>|<ipv6-address>}
```

Parameter	Description
<WORD>	Destination network name or "dynamic". The "dynamic" parameter allows you to specify a dynamic IP address for the remote endpoint. The dynamic IP address can be obtained, for example, via DHCP.
<ipv4-address>	Destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<ipv6-address>	Destination IPv6 address. The IPv6 address uses the format X:X::X:X.

Mode Interface Configuration

Examples To configure a destination IPv4 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination 192.0.3.1
```

To configure a destination IPv6 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel destination 2001:0db8::
```

To configure a destination network name for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination www.example.com
```

To configure a dynamic IP address for the tunnel destination, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel destination dynamic
```

To remove the destination address of IPSec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# no tunnel destination 192.0.3.1
```

Related commands tunnel source (IPsec)

tunnel inline-processing

Overview Use this command to configure tunnel inline-processing for an IPsec encrypted tunnel.

Tunnel inline-processing is a faster alternative to tunnel security-reprocessing which is the alternative, less efficient option. With tunnel security-reprocessing configured, the DPI engine processes incoming VPN traffic twice (before and after decryption), in order to identify incoming application traffic transported via an encrypted VPN.

Tunnel inline-processing is useful because it means packets are decrypted before being analysed and processed via the DPI engine. This is especially important for VPN traffic, where you actually want to identify application traffic transported within the IPsec VPN, rather than the outer encrypted IPsec VPN headers.

Use the **no** variant of this command to disable tunnel inline-processing for an IPsec encrypted tunnel.

Syntax

```
tunnel inline-processing
no tunnel inline-processing
```

Default Disabled

Mode Interface Configuration

Example To enable tunnel inline-processing, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel inline-processing
```

To disable tunnel inline-processing, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# no tunnel inline-processing
```

Related commands show tunnel inline-processing counters

Command changes Version 5.5.2-1.1: command added

tunnel local name (IPsec)

Overview Use this command to specify an IPSec tunnel hostname to send to the peer for authentication when you apply tunnel protection ipsec (IPsec) to encrypt the packets and configure an ISAKMP key.

Use the **no** variant of this command to remove a previously configured IPSec tunnel hostname.

Syntax

```
tunnel local name <local-name>
no tunnel local name
```

Parameter	Description
<local-name>	Source tunnel hostname.

Default The default tunnel local name is the IP address of tunnel source.

Mode Interface Configuration

Examples To configure the tunnel local name office1 for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel local name office1
```

To remove a configured tunnel local name for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel local name
```

Related commands tunnel remote name (IPsec)

tunnel local selector

Overview Use this command to specify a local subnet for a traffic selector pair.

Use the **no** variant of this command to unset the local subnet for the traffic selector pair so that it matches all sources, i.e. 0.0.0.0/0 or ::/0 for IPv4 and IPv6, respectively. When local and remote subnets for a traffic selector pair are both unset, the traffic selector pair is removed.

Syntax

```
tunnel local selector [<traffic-selector-ID>]
{<ipv4-subnet>|<ipv6-subnet>}
```

```
no tunnel local selector [<traffic-selector-ID>]
```

Parameter	Description
<traffic-selector-ID>	Optional traffic selector ID from 1 through 65535. The default is 1.
<ipv4-subnet>	IPv4 subnet in the format A.B.C.D/M.
<ipv6-subnet>	IPv6 subnet in the format of X:X::X:X/M

Default When no traffic selector pairs are configured there is an implicit traffic selector pair, where the local and remote subnets are 0.0.0.0/0 or ::/0 depending on the tunnel IPsec mode.

Mode Interface configuration

Usage notes A traffic selector pair is an agreement between IKE peers to permit traffic through a tunnel if the traffic matches a specified pair of local and remote subnets. When the local selector is specified but the remote selector is not, the selector pair implicitly matches all destinations.

Examples To specify an IPv4 destination address as the traffic selector for the traffic to match for tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth0
awplus(config-if)# tunnel destination 10.0.0.2
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel local selector 192.168.1.0/24
awplus(config-if)# tunnel remote selector 192.168.2.0/24
```

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 192.168.1.0/24
awplus(config-if)# tunnel remote selector 5 192.168.2.0/24
```

To specify an IPv6 source address as the traffic selector for the traffic to match for `tunnel0`, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth0
awplus(config-if)# tunnel destination 2001:db8:10::1
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel local selector 2001:db8:1::/64
awplus(config-if)# tunnel remote selector 2001:db8:2::/64
```

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 2001:db8:1::/64
awplus(config-if)# tunnel remote selector 5 2001:db8:2::/64
```

To unset the destination traffic selector for the traffic selector pair with ID 1, for tunnel 6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel remote selector
```

or

```
awplus(config-if)# no tunnel remote selector 1
```

Related commands

tunnel remote selector

tunnel selector paired

show interface tunnel (IPsec)

tunnel mode ipsec

Overview Use this command to configure the encapsulation tunneling mode to use.

Use the **no** variant of this command to remove an established tunnel.

Syntax

```
tunnel mode ipsec {ipv4|ipv6}
no tunnel mode
```

Parameter	Description
`ipsec ipv4`	IPv4 IPsec tunnel
`ipsec ipv6`	IPv6 IPsec tunnel

Default Virtual tunnel interfaces have no mode set.

Mode Interface Configuration

Usage notes A tunnel will not become operational until it is configured with this command.

Examples To configure IPSec in IPv4 tunnel mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel mode ipsec ipv4
```

To remove the configured IPSec tunnel mode for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel mode
```

tunnel oper-status-control

Overview Use this command to configure the control of operation status for point-to-point IPsec protected tunnels. This type of tunnel can be configured to use the presence or absence of an IPsec SA to determine if the interface should be considered 'UP' or 'DOWN'.

Use the **no** variant of this command to return a tunnel to the default configuration of not using the existence of an IPsec SA to set the oper-status of the tunnel.

Syntax

```
tunnel oper-status-control {ipsec|none}
no tunnel oper-status-control
```

Parameter	Description
ipsec	Use the presence or absence of an IPsec SA, associated with an IPsec-protected tunnel to control the oper-status of the tunnel interface.
none	Always show the oper-status of the tunnel as 'Link is UP' and 'RUNNING'.

Default None.

Mode Interface Configuration

Usage notes By default, when a tunnel is fully configured and is administratively enabled, the tunnel always shows 'Link is UP' and the RUNNING flag is always set in the output of the **show interface** command. This is because tunnels are virtual interfaces that have no electrical state associated with them. However, this does not mean that the tunnel is capable of passing traffic.

In order to provide a kind of oper-status for point-to-point IPsec protected tunnels, the tunnel can be configured to use the presence or absence of an IPsec SA to determine if the interface should be considered 'UP' or 'DOWN', respectively. When configured in this way the device will always attempt to maintain an IPsec SA with the remote device, whereas normally one would only be established if there is traffic that needs to be passed. This is necessary, otherwise routes over the tunnel would not be considered active.

Example To use the presence of IPsec SA's to control the oper-status of interface 'tunnel1', use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# tunnel oper-status-control ipsec
```

Output 1 Figure 32-17: Example output from **show interface tunnel1**

In this first example, there is an IPsec SA (i.e. IPsec has negotiated and is ready to send data) and so the link shows as 'UP'.

```
awplus#show interface tunnel1
Interface tunnel1
  Link is UP, administrative state is UP
  Hardware is Tunnel
  IPv4 address 10.1.1.1/24 point-to-point 10.1.1.255
  index 17 metric 1 mtu 1438
  UP,POINT-TO-POINT,RUNNING,MULTICAST
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Tunnel source eth1 (172.16.1.1), destination 172.16.1.2
  Tunnel name local 172.16.1.1, remote 172.16.1.2
  Tunnel traffic selectors (ID, local, remote)
    1    0.0.0.0/0                  0.0.0.0/0
  Tunnel protocol/transport ipsec ipv4, key disabled, sequencing disabled
  Checksumming of packets disabled, DF bit set, path MTU discovery disabled
  Tunnel protection via IPsec (profile "default")
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 0, bytes 0, dropped 0, multicast packets
    output packets 0, bytes 0, multicast packets 0, broadcast packets 0
    input average rate : 30 seconds 0 bps, 5 minutes 0 bps
    output average rate: 30 seconds 0 bps, 5 minutes 0 bps
  Time since last state change: 0 days 00:00:49
...
```

Output 2 Figure 32-18: Example output from **show interface tunnel1**

In the second example there is no IPsec SA and so the link is 'DOWN'.

```
awplus#show interface tunnel1
Interface tunnel1
  Link is DOWN, administrative state is UP
  Hardware is Tunnel
  IPv4 address 10.1.1.1/24 point-to-point 10.1.1.255
  index 17 metric 1 mtu 1438
  UP,POINT-TO-POINT,MULTICAST
  SNMP link-status traps: Disabled
  Bandwidth 1g
  Tunnel source eth1 (172.16.1.1), destination 172.16.1.2
  Tunnel name local 172.16.1.1, remote 172.16.1.2
  Tunnel traffic selectors (ID, local, remote)
    1    0.0.0.0/0                  0.0.0.0/0
  Tunnel protocol/transport ipsec ipv4, key disabled, sequencing disabled
  Checksumming of packets disabled, DF bit set, path MTU discovery disabled
  Tunnel protection via IPsec (profile "default")
  Router Advertisement is disabled
  Router Advertisement default routes are accepted
  Router Advertisement prefix info is accepted
    input packets 0, bytes 0, dropped 0, multicast packets
    output packets 0, bytes 0, multicast packets 0, broadcast packets 0
    input average rate : 30 seconds 0 bps, 5 minutes 0 bps
    output average rate: 30 seconds 0 bps, 5 minutes 0 bps
  Time since last state change: 0 days 00:00:49
...
```

Related commands show interface

Command changes Version 5.5.1-2.1: command added

tunnel protection ipsec (IPsec)

Overview Use this command to enable IPsec protection for packets encapsulated by this tunnel.

Use the **no** variant to disable IPsec protection.

Syntax

```
tunnel protection ipsec [profile <profile_name>]
no tunnel protection ipsec
```

Default IPsec protection for packets encapsulated by tunnel is disabled. If no custom profile is specified, the default profile is used.

Parameter	Description
<profile_name>	Custom profile name. You can use the crypto ipsec profile command to create custom profiles.

Mode Interface Configuration

Usage notes IPsec mode tunnels (IPv4 and IPv6) require this command for them to work. GRE IPv6 and L2TPv3 IPv6 tunnel have IPsec protection as an option.

Examples To enable IPsec protection by using default profile, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# tunnel protection ipsec
```

To enable IPsec protection by using a custom profile, use the following commands:

```
awplus(config)# interface tunnel14
awplus(config-if)# tunnel protection ipsec profile
my_profile
```

To disable IPsec protection for packets encapsulated by `tunnel14`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel14
awplus(config-if)# no tunnel protection ipsec
```

Related commands crypto ipsec profile

tunnel remote name (IPsec)

Overview Use this command to specify a tunnel remote name to authenticate the tunnel's remote peer device when you apply tunnel protection ipsec (IPsec) to encrypt the packets and configure an ISAKMP key.

Use the **no** variant of this command to remove a previously configured tunnel remote name.

Syntax

```
tunnel remote name <remote-name>
no tunnel local name
```

Parameter	Description
<remote-name>	Destination tunnel hostname

Default The default tunnel remote name is the IP address of tunnel destination.

Mode Interface Configuration

Examples To configure tunnel remote name office2 for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# tunnel remote name office2
```

To remove a configured tunnel local name for tunnel6, use the commands below:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel remote name
```

Related commands tunnel local name (IPsec)

tunnel remote selector

Overview Use this command to specify a destination subnet for a traffic selector pair.

Use the **no** variant of this command to unset the remote subnet for a traffic selector pair so that it matches all destinations, i.e. 0.0.0.0/0 or ::/0 for IPv4 and IPv6, respectively. When local and remote subnets for a traffic selector pair are both unset, the traffic selector pair is removed.

Syntax

```
tunnel remote selector [<traffic-selector-ID>]
{<IPv4-subnet>|<IPv6-subnet>}
```

```
no tunnel remote selector [<traffic-selector-ID>]
```

Parameter	Description
<traffic-selector-ID>	Traffic selector ID from 1 through 65535. If not specified the default value 1 is used.
<ipv4-subnet>	IPv4 subnet in the format A.B.C.D/M.
<ipv6-subnet>	IPv6 subnet in the format of X:X::X:X/M

Default When no traffic selector pairs are configured there is an implicit traffic selector pair, where the local and remote subnets are 0.0.0.0/0 or ::/0 depending on the tunnel IPsec mode.

Mode Interface configuration

Usage notes A traffic selector pair is an agreement between IKE peers to permit trafic through a tunnel if the traffic matches a specified pair of local and remote subnets. When the remote selector is specified but the local selector is not, the selector pair implicitly matches all sources.

Examples To specify an IPv4 destination address as the traffic selector for the traffic to match for tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth0
awplus(config-if)# tunnel destination 10.0.0.2
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel local selector 192.168.1.0/24
awplus(config-if)# tunnel remote selector 192.168.2.0/24
```

When no traffic selector ID is specified the default ID value is used. By specifying a traffic selector ID, additional selector pairs can be configured.

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 192.168.1.0/24
awplus(config-if)# tunnel remote selector 5 192.168.2.0/24
```

To specify an IPv6 source address as the traffic selector for the traffic to match for tunnel0, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel source eth0
awplus(config-if)# tunnel destination 2001:db8:10::1
awplus(config-if)# tunnel local name office
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel local selector 2001:db8:1::/64
awplus(config-if)# tunnel remote selector 2001:db8:2::/64
```

To configure an additional source and destination traffic selector pair for the traffic to match for tunnel0, use the commands:

```
awplus(config-if)# tunnel local selector 5 2001:db8:1::/64
awplus(config-if)# tunnel remote selector 5 2001:db8:2::/64
```

To unset the destination traffic selector for the traffic selector pair with ID 1, for tunnel6, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel6
awplus(config-if)# no tunnel remote selector
```

or

```
awplus(config-if)# no tunnel remote selector 5
```

Related commands

tunnel local selector

tunnel selector paired

show interface tunnel (IPsec)

tunnel security-reprocessing

Overview Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

Syntax

```
tunnel security-reprocessing
no tunnel security-reprocessing
```

Default Security reprocessing is disabled by default.

Mode Global Configuration

Usage notes Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the Internet Protocol Security (IPsec) Feature Overview and_Configuration Guide.

Example To enable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# no tunnel security-reprocessing
```

Related commands show interface tunnel (IPsec)

Command changes Version 5.4.8-0.2: command added

tunnel selector paired

Overview Use this command when multiple selector pairs are configured. This command forces ISAKMP to use strict pairing and therefore create separate Phase 2 IPsec SAs between pairs of source and destination selectors, based on selector ID.

Use the **no** variant of this command to stop forcing strict selector ID pairing.

Syntax
```
tunnel selector paired
```

Default Disabled

Mode Interface mode for a tunnel

Usage notes When this command is disabled, if you specify address selectors, the tunnel can permit any combination of matching sources and/or destinations. While this conforms to the RFC, it may not be the expected behavior and may cause the IPsec SA to either fail negotiation or fail to pass traffic correctly.

This command forces ISAKMP to create individual IPsec SAs for each pair of source and destination selectors that have the same selector ID. Only traffic that matches a selector pair is permitted to flow via the associated SA.

Example To create a tunnel between 172.16.1.0/24 and 172.16.2.0/24, and also between 172.16.1.0/24 and any other destination, use the following tunnel selector commands:

```
awplus# configure terminal
awplus(config)# interface tunnel0
awplus(config-if)# tunnel local selector 2 172.16.1.0/24
awplus(config-if)# tunnel remote selector 2 172.16.2.0/24
awplus(config-if)# tunnel local selector 3 172.16.1.0/24
awplus(config-if)# tunnel remote selector 3 0.0.0.0/0
awplus(config-if)# tunnel selector paired
```

Related commands
tunnel local selector

tunnel remote selector

show interface tunnel (IPsec)

Command changes Version 5.4.8-1.1: command added

tunnel source (IPsec)

Overview Use this command to specify an IPv4 or IPv6 source address or interface name for packets being encapsulated in the IPsec tunnel. The source address should be an existing IPv4 address or IPv6 address or interface name configured for an interface.

Use the **no** variant of this command to remove a tunnel source address for a tunnel interface.

Syntax

```
tunnel source {<interface-name>|<ipv4-address>|<ipv6-address>}
no tunnel source
{<interface-name>|<ipv4-address>|<ipv6-address>}
```

Parameter	Description
<interface-name>	Interface name.
<ipv4-address>	The IPv4 address uses the format A.B.C.D.
<ipv6-address>	The IPv6 address uses the format X:X::X:X.

Mode Interface Configuration

Examples To configure a source IPv4 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel source 192.168.1.1
```

To configure a source IPv6 address for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv6
awplus(config-if)# tunnel source 2001:db8::
```

To configure a source interface for IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# tunnel mode ipsec ipv4
awplus(config-if)# tunnel source eth0
```

To remove the source address of IPsec tunnel45, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel45
awplus(config-if)# no tunnel source 192.168.1.1
```

Related commands tunnel destination (IPsec)

undebug isakmp

Overview Use this command to disable debugging ISAKMP.

To enable debugging ISAKMP, see debug isakmp.

Syntax

```
undebug [crypto] isakmp [info|trace|all]
```

Parameter	Description
`undebug`	Disable debugging function.
`crypto`	Security specific command.
`isakmp`	Internet Security Association Key Management Protocol provides a common framework for key management implementations.
`info`	Informational debug messages such as protocol events.
`trace`	Verbose debug messages including protocol events and message traces.
`all`	All debug enabled.

Mode Privileged Exec

Related commands

debug isakmp

no debug isakmp

version (ISAKMP)

Overview Use this command to set the ISAKMP protocol version.

Use the **no** variant to set the protocol version to default (IKEv2).

Syntax

```
version {1 mode {aggressive|main}|2}
no version
```

Parameter	Description
1	IKEv1
main	IKEv1 Main mode. An IKE session begins with the initiator and recipient sending three two-way exchanges to define what encryption and authentication protocols are acceptable, how long keys should remain active, and whether perfect forward secrecy should be enforced. Main mode uses more packets for the process than Aggressive mode, but Main mode is considered more secure.
aggressive	IKEv1 Aggressive mode. The initiator and recipient accomplish the same objectives, but in only two exchanges.
2	IKEv2

Default If you do not specify the version, the default version is IKEv2

Mode IPsec ISAKMP Configuration

Examples To set the ISAKMP protocol version of profile "my_profile" to IKEv1 main mode, use the following commands:

```
awplus(config)# configure isakmp profile my_profile
awplus(config-isakmp-profile)# version 1 mode main
```

To set the version to its default, use the following command:

```
awplus# no version
```

Related commands crypto isakmp profile

Validation Commands show isakmp profile

33 L2TPv3 Ethernet Pseudowire Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure L2TPv3 Ethernet pseudowires.

For introductory information about L2TPV3 in AlliedWare Plus, including overview and configuration information, see the L2TPv3 Ethernet Pseudowire Feature Overview and Configuration Guide.

Command List

- "interface tunnel (L2TPv3)" on page 1139
- "l2tp unmanaged port" on page 1140
- "show interface tunnel (L2TPv3)" on page 1141
- "tunnel destination (L2TPv3)" on page 1142
- "tunnel df" on page 1144
- "tunnel local id" on page 1145
- "tunnel mode l2tp v3" on page 1146
- "tunnel protection ipsec" on page 1147
- "tunnel remote id" on page 1148
- "tunnel security-reprocessing" on page 1149
- "tunnel source (L2TPv3)" on page 1150

interface tunnel (L2TPv3)

Overview Use this command to create a tunnel interface or to enter Interface mode to configure an existing tunnel. Tunnel interfaces are identified by an index identifier that is an integer in the range from 0 through 65535.

Use the **no** variant of this command to remove a previously created tunnel interface.

Syntax

```
interface tunnel<0-65535>
no interface tunnel<tunnel-index>
```

Parameter	Description
<0-65535>	Specify a tunnel interface index identifier in the range from 0 through 65535.

Default Tunnel interfaces do not exist.

Mode Global Configuration

Usage notes After you have created the tunnel interface, use the **tunnel mode** command to enable the tunnel.

Examples To configure a tunnel interface with index 30 and enable L2TPv3 mode, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel30
awplus(config-if)# tunnel mode l2tp v3
```

To remove the tunnel interface tunnel30, use the commands:

```
awplus# configure terminal
awplus(config)# no interface tunnel30
```

Related commands show interface tunnel (L2TPv3)

tunnel mode l2tp v3

Command changes Version 5.4.7-2.1: increased range for **tunnel** index identifiers.

l2tp unmanaged port

Overview Use this command to set the UDP port for an (IPv4 and IPv6) unmanaged L2TP tunnel (L2TPv3 Ethernet Pseudowires).

This command can only change the UDP port when there is no unmanaged L2TP tunnel (L2TPv3 Ethernet Pseudowires) configured.

Use the **no** variant of this command to reset the UDP port to the default (1701).

Syntax

```
l2tp unmanaged port [<1-65535>]
no l2tp unmanaged port
```

Parameter	Description
<1-65535>	The number of the UDP port to use for an unmanaged L2TP tunnel (L2TPv3 Ethernet Pseudowires).

Default The UDP port is 1701 by default.

Mode Global Configuration

Usage notes The default UDP port for both unmanaged and managed L2TP tunnels is 1701. If both kinds of tunnel will be configured, the UDP port for the unmanaged tunnel must be changed to a different port by using the **l2tp unmanaged port** command.

Be aware of potential clashes with other UDP port users. Unless it is likely to be used for other purposes, we recommend configuring UDP port 1702 as a suitable alternative.

Example To set the UDP port for an L2TP unmanaged tunnel (L2TPv3 Ethernet Pseudowires) to 1702, use the following commands:

```
awplus# configure terminal
awplus(config)# l2tp unmanaged port 1702
```

Related commands tunnel mode l2tp v3

show running-config

show interface tunnel (L2TPv3)

Overview Use this command to display status information of a tunnel.

Syntax

```
show interface tunnel<0-65535>
```

Parameter	Description
<0-65535>	Specify a tunnel index in the range from 0 through 65535.

Mode Privileged Exec

Examples To display status information for L2TPv3 tunnel tunnel20, use the command.

```
awplus#show interface tunnel20
```

Output Figure 33-1: Example output from **show tunnel interface** on the console.

```
awplus#show interface tunnel20
Interface tunnel20
 Link is UP, administrative state is UP
 Hardware is Tunnel
 IPv4 address 192.168.10.1/24 broadcast 192.168.10.255
 IPv6 address 2001:db8:10::1/64
 IPv6 address fe80::5054:d4ff:fe84:d1aa/64
 index 16795714 metric 1 mtu 1480
 arp ageing timeout 300
 <UP,BROADCAST,RUNNING,MULTICAST>
 SNMP link-status traps: Disabled
 Tunnel source 192.168.1.1, destination 192.168.1.2
 Tunnel name local 192.168.1.1, remote 192.168.1.2
 Tunnel ID local 66, remote 77
 Tunnel protocol/transport l2tp v3, key disabled, sequencing
disabled
 Tunnel TTL inherit
 Checksumming of packets disabled, path MTU discovery disabled
 input packets 0, bytes 0, dropped 0, multicast packets 0
 output packets 5, bytes 366, multicast packets 0 broadcast
packets 0
 Time since last state change: 0 days 00:00:24
```

Related commands interface tunnel (L2TPv3)

tunnel destination (L2TPv3)

Overview Use this command to specify a tunnel destination for the remote end of the tunnel. Tunnel destination can be specified by using a destination network name or an IPv4 address.

Use the **no** variant of this command to remove a configured tunnel destination.

Syntax

```
tunnel destination {<ipv4-addr>|<destination-network-name>}
no tunnel destination
```

Parameter	Description
<ipv4-addr>	Specify the tunnel destination IPv4 address in the dotted decimal format A.B.C.D. The endpoints of the tunnel must be configured by mirroring IP addresses, that is, the tunnel source on one endpoint must be specified as the tunnel destination on the other endpoint.
<destination-network-name>	Destination network name. If the destination network name cannot be resolved, then the L2TPv3 tunnel remains inactive.

Mode Interface Configuration

Examples To configure an IPv4 tunnel destination by using an IPv4 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel destination 2.2.2.2
```

To configure an L2TPv3 tunnel destination by using a destination network name, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel destination
corporate_lan.example.com
```

To remove a tunnel destination, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel40
awplus(config-if)# no tunnel destination
```

Related commands

interface tunnel (L2TPv3)

tunnel mode l2tp v3

tunnel source (L2TPv3)

tunnel df

Overview Use this command to specify whether the DF (Don't Fragment) bit in the IP header should be set or not on outgoing packets from L2TPv3 tunnels.

Use the **no** variant of this command to return to the default setting.

Syntax

```
tunnel df {set|clear}
no tunnel df
```

Parameter	Description
`set`	Set the DF bit in the outer header
`clear`	Clear the DF bit in the outer header

Default The DF bit is **set** on all outgoing packets.

Mode Interface Configuration

Usage notes This command gives you the opportunity to clear the DF bit allowing packets greater than the MTU to be fragmented and transmitted via the L2TPv3 Ethernet pseudo-wire. This may be necessary if an L2TPv3 tunnel is connected to a bridge and MTU-exceeded messages cannot be sent back to clients.

NOTE: *If fragmentation of larger packets occurs as a result of setting the tunnel Do Not Fragment bit to clear, this may slightly increase latency of the associated traffic flow traversing the VPN, due to the fragmentation and re-assembly that occurs.*

Example To specify the DF bit on the L2TPv3 tunnel (tunnel2), use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel df clear
```

To set the DF bit on the L2TPv3 tunnel (tunnel2) back to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# no tunnel df
```

Related commands tunnel mode l2tp v3

Command changes Version 5.4.9-1.1: command added

tunnel local id

Overview This command specifies a tunnel local identifier sent to the peer to match.

Use the **no** variant of this command to remove the tunnel local ID.

Syntax

```
tunnel local id <1-2147483647>
no tunnel local id
```

Parameter	Description
<1-2147483647>	Tunnel ID from 1 through 2147483647

Default No tunnel local ID is set.

Mode Interface Configuration

Usage notes The endpoints of the tunnel must be configured by mirroring tunnel IDs, that is, the tunnel local ID on one endpoint must be specified as the tunnel remote ID on the other endpoint.

The local session ID defaults to the tunnel local ID and the local session ID is not configurable. A session provides the data channel in L2TPv3. There is a single pseudowire per L2TP session.

Examples To specify a tunnel local ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#tunnel mode l2tp v3
awplus(config-if)#tunnel local id 22
```

To remove the tunnel local ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#no tunnel local id
```

Related commands tunnel remote id

Validation Commands show interface tunnel (L2TPv3)

tunnel mode l2tp v3

Overview Use this command to configure the encapsulation tunneling mode.

Use the **no** variant of this command to remove an established tunnel.

Syntax

```
tunnel mode l2tp v3 [ipv6]
no tunnel mode
```

Parameter	Description
ipv6	Specify IPv6 as the delivery protocol.

Default Virtual tunnel interfaces have no mode set by default. If you specify a mode of **l2tp v3**, the delivery protocol is IPv4 unless you specify IPv6.

Mode Interface Configuration

Usage notes A tunnel will not become operational until it is configured with this command.

Examples To configure L2TPv3 as the encapsulation tunneling mode for tunnel20, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#tunnel mode l2tp v3
```

To remove the established tunnel20, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awlus(config-if)#no tunnel mode
```

Related commands

interface tunnel (L2TPv3)

show interface tunnel (L2TPv3)

tunnel df

tunnel protection ipsec

Overview Use this command to optionally enable IPsec protection for packets encapsulated by this tunnel.

Use the **no** variant of this command to disable IPsec protection.

Syntax

```
tunnel protection ipsec [profile <ipsec-profile>]
no tunnel protection ipsec
```

Parameter	Description
<ipsec-profile>	The name of an optional custom IPsec profile (crypto ipsec profile command) to use to protect this tunnel.

Default IPsec protection for packets encapsulated by tunnel is disabled.

Mode Interface Configuration

Usage notes You also need to configure a pre-shared key in conjunction with this command. See the crypto isakmp key command for more information about configuring the pre-shared key.

Examples To enable IPsec protection for packets encapsulated by tunnel114, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel114
awplus(config-if)#tunnel protection ipsec
```

To disable IPsec protection for packets encapsulated by tunnel114, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel114
awplus(config-if)#no tunnel protection ipsec
```

Related commands

crypto ipsec profile

crypto isakmp key

show isakmp key (IPsec)

tunnel remote id

Overview This command specifies a tunnel remote identifier sent to the peer for match.

Use the **no** variant of this command to remove the tunnel remote ID.

Syntax

```
tunnel remote id <1-2147483647>
no tunnel remote id
```

Parameter	Description
<1-2147483647>	Tunnel ID from 1 through 2147483647

Default No tunnel remote ID is set.

Mode Interface Configuration

Usage notes The endpoints of the tunnel must be configured by mirroring tunnel IDs, that is, the tunnel remote ID on one endpoint must be specified as the tunnel local ID on the other endpoint.

The remote session ID defaults to the tunnel remote ID and the remote session ID is not configurable. A session provides the data channel in L2TPv3. There is a single pseudowire per L2TP session.

Examples To specify a tunnel remote ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#tunnel mode l2tp v3
awplus(config-if)#tunnel remote id 22
```

To remove the tunnel remote ID, use the commands:

```
awplus#configure terminal
awplus(config)#interface tunnel20
awplus(config-if)#no tunnel remote id
```

Related commands tunnel local id

Validation Commands show interface tunnel (L2TPv3)

tunnel security-reprocessing

Overview Use this command to enable stream security reprocessing on all tunnel interfaces.

Use the **no** variant of this command to disable security reprocessing on all tunnel interfaces.

Note that tunnel security reprocessing increases the load on your device and reduces throughput. This is because traffic is processed twice through the DPI engine. Therefore, it should only be enabled if your solution requires it.

Syntax

```
tunnel security-reprocessing
no tunnel security-reprocessing
```

Default Security reprocessing is disabled by default.

Mode Global Configuration

Usage notes Use this command when you need to reinspect the traffic in a tunnel terminating on the device using stream UTM features after tunnel headers and encryption have been removed. For a configuration example using this command, see the Internet Protocol Security (IPsec) Feature Overview and_Configuration Guide.

Example To enable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# tunnel security-reprocessing
```

To disable security reprocessing, use the commands:

```
awplus# configure terminal
awplus(config)# no tunnel security-reprocessing
```

Related commands show interface tunnel (IPsec)

Command changes Version 5.4.8-0.2: command added

tunnel source (L2TPv3)

Overview Use this command to specify a tunnel source for the tunnel interface. The tunnel source can be specified by using an interface name or an IPv4 address. The source address must be an existing IPv4 address configured for an interface.

Use the **no** variant of this command to remove a tunnel source for a tunnel interface.

Syntax

```
tunnel source {<ipv4-addr>|<interface-name>}
no tunnel source
```

Parameter	Description
<ipv4-addr>	Specify the tunnel source IPv4 address for the tunnel interface in the dotted decimal format A.B.C.D. The endpoints of the tunnel must be configured by mirroring IP addresses, that is, the tunnel source on one endpoint must be specified as the tunnel destination on the other endpoint.
<interface-name>	Available interface name. Any AlliedWare Plus interface type (eth, vlan, ppp, tunnel, lo, etc). Using interface name can minimize the number of user-configured IP addresses and allow the tunnel source IP address to be dynamically issued via, for example, DHCP.

Mode Interface Configuration

Examples To configure an L2TPv3 tunnel source IPv4 address, use the commands:

```
awplus# configure terminal
awplus# interface eth0
awplus(config-if)# ip address 1.1.1.1/24
awplus(config-if)# interface tunnel1
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel source 1.1.1.1
```

To use an interface name as the tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel2
awplus(config-if)# tunnel mode l2tp v3
awplus(config-if)# tunnel source eth2
```

To remove a tunnel source, use the commands:

```
awplus# configure terminal
awplus(config)# interface tunnel1
awplus(config-if)# no tunnel source
```

Related commands

interface tunnel (L2TPv3)

tunnel destination (L2TPv3)

tunnel mode l2tp v3